

RECORD OF TRIAL²

of

(Station or Ship)

By

GENERAL

COURT-MARTIAL

Convened by _____ Commander _____

(Title of Convening Authority)

UNITED STATES ARMY MILITARY DISTRICT OF WASHINGTON

(Unit/Command of Convening Authority)

Tried at

Fort Meade, MD

(Place or Places of Trial)

on

see below

(Date or Dates of Trial)

Date or Dates of Trial:

23 February 2012, 15-16 March 2012, 24-26 April 2012, 6-8 June 2012, 25 June 2012, 16-19 July 2012, 28-30 August 2012, 2 October 2012, 12 October 2012, 17-18 October 2012, 7-8 November 2012, 27 November - 2 December 2012, 5-7 December 2012, 10-11 December 2012, 8-9 January 2013, 16 January 2013, 26 February - 1 March 2013, 8 March 2013, 10 April 2013, 7-8 May 2013, 21 May 2013, 3-5 June 2013, 10-12 June 2013, 17-18 June 2013, 25-28 June 2013, 1-2 July 2013, 8-10 July 2013, 15 July 2013, 18-19 July 2013, 25-26 July 2013, 28 July - 2 August 2013, 5-9 August 2013, 12-14 August 2013, 16 August 2013, and 19-21 August 2013.

1 Insert "verbatim" or "summarized" as appropriate. (This form will be used by the Army and Navy for verbatim records of trial only.)

2. See inside back cover for instructions as to preparation and arrangement.

3.7 COTS Software Sites

- 3D analyst (ArcGlobe)
 - <http://www.esri.com/software/arcgis/extensions/3danalyst/index.html>
- Acrobat Reader
 - <http://www.adobe.com>
 - <http://www.esri.com>
- Analyst Notebook
 - <http://www.i2.co.uk>
- Java
 - <http://java.sun.com/>
- Microsoft
 - <http://www.microsoft.com/>
- Netscape
 - <http://www.netscape.com/>
- Roxio
 - <http://roxio.com>
- Symantec
 - <http://www.symantec.com/index.htm>
- Winzip
 - <http://www.winzip.com/>
- WS_FTP
 - <http://www.ipswitch.com/>

3.8 Hardware Description

The following is a list of DCGS-A V3.1 P3 BALs hardware information:

Alienware Laptop - Model A51M	3.8 GHz, 2GB RAM memory, 17" display with high resolution graphics.
Dell Laptop - Model M90	2.33 GHz Intel Dual Processor Core, 3.25GB RAM memory, 93.1 GB hard drive, with NVIDIA graphics card, DCD-RW Optical Drive, Network Interface Card and a 17 inch display with high resolution graphics.
Laptop - Model Dell M6300	2.5 GHz Intel Core 2 Duo T9300, 4GB DDR2-667 SDRAM (2 DIMM), NVIDIA Quadro FX3600M 512 MB, 160 GB 7200RPM Hard Drive, Std Touchpad, 8x DVD+/- & Roxio Creator , and a 17" wide screen WUXGA LCD.
Dell Precision 490 Workstation	1st Processor: Intel XEON DUAL CORE Processor 3.00GHZ, 2MB L2 Cache; 2nd Processor: Intel XEON DUAL CORE Processor 2.80GHZ, 2MB L2 Cache; 4GB, DDR2 ECC SDRAM Memory, 400MHZ; NVIDIA FX 4500 512MB 2 DUI OR GA 1st Hard Drive: 80GB Serial ATA 7200RPM Hard Drive w/Databurst Cache, Non-Raid, Precision 470/670; 2nd Hard Drive: 80GB Serial ATA 7200RPM Hard Drive with

	Databurst Cache Raid; Floppy Drive: 3.5, 1.44MB; 48X/32X CD-RW/DVD Combo.
Dell Precision T5400 Desk Top	1st Processor: Quad Core Xeon Proc X5450, 3.00GHz, 2X 6MB L2 Cache,1333MHz; 2nd Processor: Quad Core Xeon Proc X5450, 3.00GHz, 2X6MB L2 Cache,1333MHz, 4GB, DDR2 ECC SDRAM Memory 667MHz, 4X1GB; NVIDIA Quadro FX3700 512MB dual DVI Graphics Card; 160GB SATA, 10K RPM Hard Drive with 16MB DataBurst Cache; CD-ROM or DVD-ROM Drive: 16X DVD+/-RW.

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

Prosecution Motion

for Maximum Punishments for
Lesser Included Offenses

22 June 2012

RELIEF SOUGHT

The prosecution respectfully requests that the Court adopt the following maximum punishments for the stated lesser-included offenses:

(1) for Attempt of the 18 U.S.C. § 793(e) offenses (i.e., Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II), to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined;

(2) for Attempt of the 18 U.S.C. § 641 offenses (i.e., Specifications 4, 6, 8, 12, and 16 of Charge II), to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined;

(3) for Attempt of the 18 U.S.C. § 1030(a)(1) offenses (i.e., Specifications 13 and 14 of Charge II), to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined;

(4) for Property of a Value Less Than \$1,000 for the 18 U.S.C. § 641 offenses (i.e., Specifications 4, 6, 8, 12, and 16 of Charge II), to be dishonorably discharged from the service, to be confined for one year, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined; and

(5) for Clauses 1 and 2 of Article 134, Uniform Code of Military Justice (UCMJ), for the 18 U.S.C. § 1030(a)(1) offenses (i.e., Specifications 13 and 14 of Charge II), to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined.

BURDEN OF PERSUASION AND BURDEN OF PROOF

The burden of proof on any factual issue the resolution of which is necessary to decide a motion shall be by preponderance of the evidence. See Manual for Courts-Martial (MCM), United States, Rule for Courts-Martial (RCM) 905(c)(1) (2012). The burden of persuasion on any factual issue the resolution of which is necessary to decide a motion shall be on the moving party. See RCM 905(c)(2).

APPELLATE EXHIBIT 161
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

FACTS

On 8 June 2012, the Court ordered that it will instruct on attempt as a lesser-included offense (LIO) if raised by the evidence for Specifications 2-16 of Charge II. See Appellate Exhibit CXXXXIII, at 6.

On 8 June 2012, the Court ordered that it will instruct on property of a value less than \$1,000 as an LIO for Specifications 4, 6, 8, 12, and 16 of Charge II. See id.

On 8 June 2012, the Court ordered that it will instruct on clauses 1 and 2 of Article 134, UCMJ, as an LIO for Specifications 13 and 14 of Charge II. See id.

The language of 18 U.S.C. § 793(d) reads as follows:

Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it[.]

18 U.S.C. § 793(d) (1996).

The language of 18 U.S.C. 1030(a)(1) reads as follows:

Whoever having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated,

delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it[.]

18 U.S.C. § 1030(a)(1) (2008).

WITNESSES/EVIDENCE

The prosecution does not request any witnesses or evidence be produced for this motion. The prosecution requests that the Court consider the Appellate Exhibits referenced herein.

LEGAL AUTHORITY AND ARGUMENT

The “maximum limits for the authorized punishments of confinement, forfeitures and punitive discharge (if any) are set forth for each offense listed in Part IV of [the MCM].” RCM 1003(c)(1)(A)(i). The rule continues that “[f]or an offense not listed in Part IV of [the MCM] which is included in or closely related to an offense listed therein the maximum punishment shall be that of the offense listed[.]” RCM 1003(c)(1)(B)(i). However, for “[a]n offense not listed in Part IV and not included in or closely related to any offense listed therein[.]” that offense “is punishable as authorized by the United States Code, or as authorized by the custom of the service.” RCM 1003(c)(1)(B)(ii) (stating that “[w]hen the United States Code provides for confinement for a specified period or not more than a specified period the maximum punishment by court-martial shall include confinement for that period”). The rule concludes that “[i]f the period is 1 year or longer, the maximum punishment by court-martial also includes a dishonorable discharge and forfeiture of all pay and allowances[.]” RCM 1003(c)(1)(B)(ii).

- I: THE MAXIMUM PUNISHMENT FOR THE LIO OF ATTEMPT IS THE SAME AS THE MAXIMUM PUNISHMENT FOR THE OFFENSE ATTEMPTED.

The MCM states as follows:

Any person subject to the code who is found guilty of an attempt under Article 80 to commit any offense punishable by the code shall be subject to the same maximum punishment authorized for the commission of the offense attempted, except that in no case shall the death penalty be adjudged, nor shall any mandatory minimum punishment provisions apply; and in no case, other than attempted murder, shall confinement exceeding 20 years be adjudged.

MCM, Part IV, ¶ 4.e. Accordingly, the maximum punishment for the LIO of attempt equates to the maximum punishment for the offense attempted.

The maximum punishment for Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II in violation of 18 U.S.C. § 793(e) is a fine and/or imprisonment of ten years. See 18 U.S.C. § 793(e) (whoever violates this provision “shall be fined under this title or imprisoned not more than ten years, or both”); see also U.S. Dep’t of Army, Pam. 27-9, Military Judges’ Benchbook (1 January 2010) (3-60-2B(a)) (Benchbook) (the maximum punishment is “based on the federal statute allegedly violated”). Thus, the maximum punishment for the LIO of attempt of Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II is to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined. See RCM 1003(c)(1)(B)(ii) (stating that “[i]f the period is 1 year or longer, the maximum punishment by court-martial also includes a dishonorable discharge and forfeiture of all pay and allowances”).

The maximum punishment for Specifications 4, 6, 8, 12, and 16 of Charge II in violation of 18 U.S.C. § 641 is a fine and/or imprisonment of ten years. See 18 U.S.C. § 641 (whoever violates this provision “shall be fined under this title or imprisoned not more than ten years, or both”). Thus, the maximum punishment for the LIO of attempt of Specifications 4, 6, 8, 12, and 16 of Charge II in violation of 18 U.S.C. § 641 is to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined. See RCM 1003(c)(1)(B)(ii), *supra*.

The maximum punishment for Specifications 13 and 14 of Charge II in violation of 18 U.S.C. § 1030(a)(1) is a fine and/or imprisonment of ten years. See 18 U.S.C. § 1030(c)(1)(A) (the appropriate punishment is “a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph”). Thus, the maximum punishment for the LIO of attempt of Specifications 13 and 14 of Charge II in violation of 18 U.S.C. § 1030(a)(1) is to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined. See RCM 1003(c)(1)(B)(ii), *supra*.

II: THE MAXIMUM PUNISHMENT FOR THE LIO OF PROPERTY OF A VALUE LESS THAN \$1,000 FOR THE 18 U.S.C. § 641 OFFENSES IS ONE YEAR.

The LIO of Property of a Value Less Than \$1,000 is neither listed, nor included in or closely related to an offense listed, in the MCM. See RCM 1003(c)(1)(A)(i); see also RCM 1003(c)(1)(B)(i); see also *United States v. Leonard*, 64 M.J. 381, 383 (C.A.A.F. 2007) (observing “that the ‘closely related’ language in RCM 1003(c)(1)(B)(ii) refers to offenses that are closely related to offenses listed in the MCM”).¹ Thus, the LIO “is punishable as authorized by the United States Code[.]” RCM 1003(c)(1)(B)(ii); see also Benchbook (3-60-2B(a)) (the

¹ The LIO is not included in, or closely related to, Article 121, UCMJ, a punitive article that criminalizes larceny of only tangible items having corporeal existence and not intangibles. See Benchbook (3-46-1, n. 19); see also *United States v. Mervine*, 26 M.J. 482 (C.M.A. 1988). Thus, Article 121, UCMJ, does not criminalize the conduct underlying the LIO of Property of a Value Less Than \$1000 and, thus, is not closely related. See *United States v. Tenney*, 60 M.J. 838, 843 (N.M. Ct. Crim. App. 2005) (where the accused’s misconduct does not violate the alleged punitive article, that article is not a closely related offense).

maximum punishment is “based on the federal statute allegedly violated”). The maximum punishment for a violation of 18 U.S.C. § 641 of property of a value less than \$1,000 is a fine and/or imprisonment of one year. See 18 U.S.C. § 641 (“if the value of such property in the aggregate...does not exceed the sum of \$1,000, he shall be fined under this title or imprisoned not more than one year, or both”). Thus, the maximum punishment for the LIO of property of a value less than \$1,000 for Specifications 4, 6, 8, 12, and 16 of Charge II is to be dishonorably discharged from the service, to be confined for one year, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined. See RCM 1003(c)(1)(B)(ii), *supra*.

III: THE MAXIMUM PUNISHMENT FOR THE LIO OF CLAUSES 1 AND 2 OF ARTICLE 134, UCMJ, FOR THE 18 U.S.C. § 1030(a)(1) OFFENSES IS TEN YEARS.

The LIO of Clauses 1 and 2 of Article 134, UCMJ, for the 18 U.S.C. § 1030(a)(1) offenses is neither listed, nor included in or closely related to an offense listed, in the MCM. See RCM 1003(c)(1)(A)(i); see also RCM 1003(c)(1)(B)(i). Thus, the LIO “is punishable as authorized by the United States Code[.]” RCM 1003(c)(1)(B)(ii) (stating that “[w]hen the United States Code provides for confinement for a specified period or not more than a specified period the maximum punishment by court-martial shall include confinement for that period”). The LIO of Clauses 1 and 2 of Article 134, UCMJ, includes the conduct and *mens rea* proscribed by a directly analogous federal criminal statute, specifically 18 U.S.C. § 793(d) or 18 U.S.C. § 1030(a)(1). See Leonard, 64 M.J. at 385. Accordingly, the Court should reference the maximum punishment under 18 U.S.C. § 793(d) and 18 U.S.C. § 1030(a)(1).

The elements of the LIO of Clauses 1 and 2 of Article 134, UCMJ, are as follows: (1) that the accused did or failed to do certain acts; and (2) that, under the circumstances, the accused’s conduct was to the prejudice of good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces. See UCMJ art. 134 (2012). The language of 18 U.S.C. § 793(d) and 18 U.S.C. § 1030(a)(1) is listed above. See supra, at 2-3.

The Court of Appeals for the Armed Forces (CAAF) in Leonard is instructive on this matter. In Leonard, the appellant was convicted of wrongfully and knowingly receiving visual depictions of minors engaging in sexually explicit conduct in violation of clauses 1 and 2 of Article 134, UCMJ. The issue was whether the maximum punishment for the offense “may be determined by reference to the maximum punishment for violation of a federal statute that proscribes and criminalizes the same criminal conduct and *mens rea* included in the specification.” Id., at 381. The CAAF answered in the affirmative, finding that the criminal conduct and *mens rea* set forth in the specification described the gravamen of the offense proscribed by the analogous federal statute, 18 U.S.C. § 2252(a)(1), for which the maximum sentence was fifteen years. The CAAF did not find error in the trial court’s reference to the maximum sentence for this federal statute. See id., at 384 (focusing “on whether the offense as charged [was] ‘essentially the same,’ as that proscribed by the federal statute”).

Like in Leonard, the LIO of Clauses 1 and 2 of Article 134, UCMJ, for Specifications 13 and 14 of Charge II includes the conduct and *mens rea* proscribed by an analogous federal statute; namely, either 18 U.S.C. § 793(d) (i.e., the willful communication of information relating

to the national defense to a person not entitled to receive it with reason to believe that information could be used to the injury of the United States or to the advantage of any foreign nation) or 18 U.S.C. § 1030(a)(1) (i.e., having knowingly exceeding authorized access, and by means of such conduct having obtained information that requires protection against unauthorized disclosure for reasons for national defense or foreign relations, willfully communicate such information to a person not entitled to receive it with reason to believe such information could be used to the injury of the United States or the advantage of any foreign nation). Accordingly, the Court should reference the maximum punishment under 18 U.S.C. § 793(d) and 18 U.S.C. § 1030(a)(1).

The maximum punishment for a violation of 18 U.S.C. § 793(d) and 18 U.S.C. § 1030(a)(1) is a fine and/or imprisonment of ten years. See 18 U.S.C. § 793(d) (whoever violates this provision "shall be fined under this title or imprisoned not more than ten years, or both"); see also 18 U.S.C. § 1030(c)(1)(A) (the appropriate punishment is "a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph"). Thus, the maximum punishment for Clauses 1 and 2 of Article 134, UCMJ, the LIO of Specifications 13 and 14 of Charge II, is to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined. See RCM 1003(c)(1)(B)(ii), *supra*.

CONCLUSION

The prosecution respectfully requests that the Court adopt the following maximum punishments for the stated lesser-included offenses:

(1) for Attempt of the 18 U.S.C. § 793(e) offenses (i.e., Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II), to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined;

(2) for Attempt of the 18 U.S.C. § 641 offenses (i.e., Specifications 4, 6, 8, 12, and 16 of Charge II), to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined;

(3) for Attempt of the 18 U.S.C. § 1030(a)(1) offenses (i.e., Specifications 13 and 14 of Charge II), to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined;

(4) for Property of a Value Less Than \$1,000 for the 18 U.S.C. § 641 offenses (i.e., Specifications 4, 6, 8, 12, and 16 of Charge II), to be dishonorably discharged from the service, to be confined for one year, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined; and

(5) for Clauses 1 and 2 of Article 134, Uniform Code of Military Justice (UCMJ), for the 18 U.S.C. § 1030(a)(1) offenses (i.e., Specifications 13 and 14 of Charge II), to be dishonorably discharged from the service, to be confined for ten years, to forfeit all pay and allowances, to be reduced to Private, E-1, and to be fined.



J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 22 June 2012.



J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

UNITED STATES OF AMERICA)

v.)

Prosecution Witness List

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

22 June 2012

The prosecution may call the following witnesses to testify on the merits at trial and/or during the presentencing phase¹ of the above-captioned court-martial:

1. CDR Youssef Aboul-Enein, Defense Intelligence Agency, Bolling AFB, MD 20032, (202) 231-7737
2. SFC Paul Adkins, 10th Mountain Division (LI), Fort Drum, NY 13602, (315) 772-8620
3. Ms. Sara Loving (Alicie), Fort Drum, NY 13603, (315) 454-3185
4. Ms. Lisa Alleman, Office of Personnel Management, Boyers, PA 16016, 724-794-5612 ext 7000
5. SA Charles Ames, Europe Branch Office - Computer Crime Investigative Unit, Funari Barracks, APO AE 09008, 49-621-730-5387
6. SPC Mary Amiatu, Camp Arifjan, Kuwait, APO AE 09306, DSN 318-430-6314
7. SPC Kyra (Marshall) Amos, B Co., 57th Signal Battalion, Fort Hood, TX 76544 (Deployed to Afghanistan), (254) 287-3997
8. SFC Jose Anica, HHC, National Ground Intelligence Center (NGIC), Charlottesville, VA 22911, (434) 980-7453
9. Mr. Peter Artale, 902d MI Group, Fort Meade, MD 20755, (301) 677-5107
10. SPC Eric Baker, Fort Drum, NY 13602, (910) 354-4552
11. SPC Kimberly Bales, HHC, 2BCT, 10th Mountain Division (LI), Fort Drum, NY 13602, (315) 774-2959
12. WO1 Kyle Balonek, HHC, HHBN, 10th Mountain Division (LI), Fort Drum, NY 13602, (315) 775-7203

¹ As of the date of this filing, persons identified with an asterisk ("*") are witnesses only for purposes of the presentencing phase.

13. CW4 Anthony Barnett, US Army Intelligence Center and Center of Excellence, Fort Huachuca, AZ 85613, (520) 538-6428
14. Mr. Joseph Benthall, Watertown, NY 13601, (315) 405-8856
15. SA Troy Bettencourt, Department of Treasury, Washington, DC 20220, (571) 721-8969
16. SSG Peter Bigelow, US Army NATO, Allied Forces Command South, Naples, Italy, FPO AE 09620, (039)348-094-0656
17. Mr. Wyatt Bora, Air Force Research Laboratory, Rome, NY 13440, (315) 330-4944
18. SA John Bowen, 3rd MP Group (CID), Fort Eustis, VA 23604, (352) 516-1470
19. Mr. Steve Buchanan, Intelink, Fort Meade, MD 20755, (410) 854-9500
20. * AMB Patricia Butenis, U.S. Ambassador to Sri Lanka Duty Station: U.S. Embassy, Sri Lanka, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
21. * BG (Ret.) Robert Carr, Defense Intelligence Agency, Bolling AFB, MD 20032, (703) 695-0071
22. Mr. Sean Chamberlin, 902d MI Group, Fort Meade, MD 20755, (301) 677-3425
23. CPT Thomas Cherepko, NATO Force Command, Madrid, Spain 28223, (412) 387-3090
24. SA Charles Clapper, Arizona Branch Office - Computer Crime Investigative Unit, Fort Huachuca, AZ 85613, (520) 538-0182
25. Dr. Michael Collins, RedJack, Silver Spring, MD 20910, (301) 335-6352
26. Mr. Domingo U. Conlu, US Army Human Resources Command, Fort Knox, KY 40122, (502) 613-9990
27. SGT Lorena Cooley, HHC, 2BCT, 10th Mountain Division (LI), Fort Drum, NY 13602, (770) 853-3954
28. * Ms. Elizabeth Dibble, Principal Deputy Assistant Secretary, Bureau of Near Eastern Affairs, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
29. * Mr. Vann Van Diepen, Deputy Assistant Secretary, Bureau of International Security and Nonproliferation, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
30. Mr. Jim Downey, Defense Information Systems Agency, Fort Meade, MD 20755, (571) 205-2052

31. SA Jeremy Drews, 10740 Pearl Sands Dr, El Paso, TX 79924, (915) 568-1700
32. SA Antonio Edwards, Homeland Security Investigations, National Security Unit, Atlanta, GA 30301, (404) 346-2846
33. CW2 Joshua Ehresman, HSC, HHBN, 2d ID, Camp Red Cloud, Korea, APO AP 96258, 001-82-505-732-7619
34. SA Kirk Ellis, Rock Island Fraud Resident Agency, Major Procurement Fraud Unit, Moline, IL 61265, (309) 757-5812
35. Mr. John Feeley, Acting Principal Deputy Assistant Secretary, Bureau of Western Hemisphere Affairs, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
36. Mr. Ryan Fidler, Nacon Consulting, LLC, Annapolis, MD 21403, (410) 295-5070
37. CPT Matthew Freeburg, Fort Sill, OK 73503, (915) 588-8102
38. CPT Casey Fulton, 2BCT, 10th Mountain Division (LI), Fort Drum, NY 13602, (404) 769-8984
39. Mr. James Fung, Brookhaven National Laboratory, Upton, NY 11973, (631) 344-8403
40. Ms. Shelia Glenn, Fort Meade, MD 20755, (301) 677-3284
41. Mr. Mike Goldman, Brookhaven National Laboratory, Upton, NY 11973, (631) 344-3324
42. SA Toni Graham, Hawaii CID Office, 1314 Lyman Road, Building 3026, Schofield Barracks, HI 96857, (808) 655-1776
43. Mr. Jacob Grant, US Central Command, MacDill AFB, FL 33621, (813) 529-6068
44. Mr. Bert Haggett, HQDA G-2, Washington, DC 20310, (703) 695-2654
45. VADM Robert Harward, US Central Command, MacDill AFB, FL 33621, POC: COL Bruce Pagel, Acting SJA at bruce.pagel@centcom.mil
46. Ms. Jacqueline Haylock, Defense Military Pay Office, Fort, Myer, VA 22211, (703) 696-3125
47. Mr. Patrick Hoeffel, Intelligent Software Solutions, Inc., 2001 Jefferson Davis Hwy, Suite 909, Arlington, VA 22202, (719) 457-0232
48. Mr. Matthew Hosburgh, Westminster, CO 80021, (720) 232-6538
49. LT (US Navy) Thomas Hoskins, US Central Command, MacDill AFB, FL 33621, (813) 529-5321

50. Ms. Tina Huffman, Watertown, NY 13601, (315) 772-7163
51. Mr. George Huley, HQDA G-3/5/7, Army Pentagon, Washington, DC 20310, (703) 614-6558
52. SA Susy Hwang, Federal Bureau of Investigation, Washington, DC 20535, (202) 278-2000
53. Ms. Elisa K. (Rubin) Ivory, S2 OIC, 305th MI Battalion, US Army Intelligence Center and Center of Excellence, Fort Huachuca, AZ 85613, (520) 533-6590
54. Mr. Albert J. Janek, Management Officer, Duty Station: U.S. Embassy, Minsk, POC: Mr. John Blanck, (202) 647-7246
55. Mr. Glen Johnson, Director, Messaging Systems Office, Bureau of Information Resource Management, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
56. SA Mark Johnson, Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134, (571) 451-9326
57. AMB Tina Kaidanow, Principal Deputy Assistant Secretary, Bureau of European Affairs, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
58. * AMB Patrick F. Kennedy, Under Secretary for Management, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
59. SA Kenneth King, Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134, (571) 305-4462
60. * Mr. John Kirchoffer, Chief of Enterprise Strategies, Office of Counterintelligence (CI) Human Intelligence (HUMINT) Enterprise Management, Defense Counterintelligence and Human Intelligence Center, Defense Intelligence Agency, Bolling AFB, MD 20032, (703) 695-0071
61. * AMB Michael Kozak, Senior Adviser, Bureau of Democracy, Rights and Labor, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
62. Mr. Adrian Lamo, Carmichael, CA 95608, (916) 944-1024
63. CW5 Jon Larue, DAMO-AV, Pentagon, DC 20310, (703) 693-3579
64. Mr. Danny J. Lewis, Defense Intelligence Agency, Bolling AFB, MD 20032, (571) 305-7100
65. * Mr. Scott Liard, Chief, Counterintelligence (CI) Enterprise Management Division, Defense Counterintelligence and Human Intelligence Center, Defense Intelligence Agency, Bolling AFB, MD 20032, (703) 695-0071

66. CPT Steven Lim, HQ, 1st Army Division-East, Fort Meade, MD 20755, (301) 833-8461
67. SA Jennie Lisciandri, Okinawa CID Office, Building 220 Unit 35139, Okinawa, Japan APO AP 96376-5139, DSN (315) 644-4188
68. SGT Chad Madaras, B Co. (B Co), 2nd Brigade Special Troops Battalion (2 BSTB), 2nd Brigade Combat Team (2 BCT), 10th Mountain Division (LI), Fort Drum, NY 13602, (315) 404-6275
69. Mr. Brian Madrid, Buckeye, AZ 85326, (602) 390-1285
70. Ms. Tamara Mairena, Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134, (571) 305-4478
71. LTC Stanley Malloy, US Army Cyber Command, Fort Belvoir, VA 22060, (703) 806-4691
72. SA Mark Mander, Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134, (571) 305-4463
73. SGT Alejandro Marin, 800th MP Brigade, Uniondale, NY 11553, (516) 946-7366
74. Mr. Randy Marks, Intelink, Fort Meade, MD 20755, (410) 654-9500
75. * Mr. James McCarl, Chief, Mission Intergration Division, Joint IED Defeat Organization (JIEDDO), Army Pentagon, Washington DC 20310, (877) 251-3337
76. Mr. Vince McCarron, HQDA G-2, Washington, DC 20310, (703) 614-6440
77. Mr. Brian Mcfall, US Central Command, MacDill AFB, FL 33621, (716) 830-8545
78. Mr. James McManus, Brookhaven National Laboratory, Upton, NY 11973, (631) 344-4107
79. COL David Miller, BDE Modernization Command, Fort Bliss, TX, (915) 568-4250
80. Mr. Jason Milliman, Palmyra, VA 22963, (434) 995-4441
81. Mr. James Moore, Deputy Assistant Secretary, Bureau of South and Central Asian Affairs, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
82. Mr. Ken Moser, US Central Command, MacDill AFB, FL 33621, (813) 529-0302
83. Mr. Jeffery Motes, JTF-GTMO, Guantanamo Bay, Cuba, 011-5399-9805
84. Mr. Troy Moul, US Army Intelligence Center and Center of Excellence, Fort Huachuca, AZ 85613, (520) 538-6767

85. * Mr. Kin Moy, Deputy Assistant Secretary, Bureau of East Asian and Pacific Affairs, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
86. Mr. Jonathan Muldoon, DISA, Pensacola, FL 32508, (850) 452-7797
87. * AMB Stephen Mull, Executive Secretary, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
88. Mr. Nicholas Murphy, Reviewer, Office of Global Information Services, Bureau of Administration, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
89. Lt Col (R) Martin Nehring, US Central Command, MacDill AFB, FL 33621, (805) 443-7669
90. MAJ Katherine Ogletree, Student, CGSC, Fort Belvoir, VA 22060 (until OCT, then NIU at Bolling AFB), (443) 640-5754
91. SGT Daniel Padgett, Fort Leavenworth, KS 66027, (209) 681-3608
92. AMB David Pearce, Deputy Special Representative for Afghanistan and Pakistan, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
93. Mr. H. Dean Pittman, Principal Deputy Assistant Secretary, Bureau of International Organization Affairs, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
94. * Lt Col Robert Pope, US Central Command, MacDill AFB, FL 33621, (813) 529-5165
95. SSG Adam Price, HHC, 2BCT, 10th Mountain Division (LI), Fort Drum, NY 13602, (808) 489-0852
96. SA Calder Robertson, Europe Branch Office - Computer Crime Investigative Unit, Funari Barracks, APO AE 09008, DSN 314-380-5355
97. * LTC Rodney Roberts, US Central Command, MacDill AFB, FL 33621, (813) 529-5130
98. Ms. Theresa Robinson, Chambersburg, PA 17201, (717) 267-5696
99. SA Ronald Rock, Diplomatic Security Service, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
100. CW4 Armond Rouillard, G33, US Army Network Enterprise Technology Command, Fort Belvoir, VA 22060, (254) 291-8968
101. SGT David Sadtler, 709th MI BN, Harrogate, UK, APO AE 09468, 01423-677-467

102. Mr. Doug Schasteen, Wilco Technologies, Inc., 4125 Broadway, Suite 200, Kansas City, MO 64106, 816-842-6262 x 158
103. Ms. Jacqueline Scott, US Central Command, MacDill AFB, FL 33621, (813) 529-6670
104. AMB Stephen Seche, Deputy Assistant Secretary, Bureau of Near Eastern Affairs, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
105. SAC David Shaver, Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134, (571) 305-4481
106. Ms. Jihreah Showman, Hope Mills, NC 28348, (918) 935-4185
107. SA Thomas Smith, USACIDC, Fort Gordon, GA 30905, (706) 791-2020
108. SA Mitchell Song, Federal Bureau of Investigation, Washington, DC 20535, (202) 278-4478
109. CPT Loren Stark, HHB, 1-37 FA, 3SBCT, 2nd Infantry Division, Fort Lewis, WA (Deployed to Afghanistan), (303) 551-5760
110. Mr. Ralph Steinway, HQDA, G-1 (DAPE-MPT), Pentagon, DC 20310, (703) 695-5914
111. SA George Street, Chief, Operations Support Division G2X, 902d MI Monterey Field Office, Monterey, CA, (703) 706-2905
112. Ms. Cathryn Strobl, Central Intelligence Agency, McLean, VA 22101, POC: Mr. Brian G., (703) 874-7601
113. * Ms. Susan Swart, Chief Information Officer, Bureau of Information Resource Management, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
114. Ms. Tasha Thian, Agency Records Officer, Office of Global Information Services, Bureau of Administration, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
115. SSG Robert Thomas, III, HHT, Support Squadron, 3d ACR, Fort Hood, TX, (254) 833-1705
116. Mr. Louis Travieso, US Central Command, MacDill AFB, FL 33621, (813) 827-1163
117. Mr. Charles Vankleek, US Central Command, MacDill AFB, FL 33621, (813) 529-6694
118. * Ms. Shari Villaros, Deputy Coordinator for Regional Affairs, Bureau of Counter Terrorism, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246

119. SFC Garrih Walker, HHC, 2 BSTB, 10th Mountain Division, (LI), Fort Drum, NY 13602, (315) 772-7946
120. Mr. Greg Weaver, Compliance Branch Chief, US Army Cyber Command, Fort Belvoir, VA, (703) 806-4691
121. Ms. Florinda White, CERDEC Software Engineering Directorate, Aberdeen Proving Ground, MD 21005, (443) 867-3783
122. SA John Wilbur, Department of Treasury, Washington, DC 20220, (202) 622-8952
123. SA Alfred Williamson, Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134, (571) 305-4488
124. Mr. Charlie Wisecarver, Office of Global Information Services, Bureau of Administration, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
125. Mr. Alex Withers, Brookhaven National Laboratory, Upton, NY 11973, (631) 344-7723
126. RDML David Woods, Commander, JTF-GTMO, Guantanamo Bay, Cuba, POC: CDR T. Welsh, DSN 660-9911
127. AMB Don Yamamoto, Principal Deputy Assistant Secretary, Bureau of African Affairs, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246
128. SA Garon Young, Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134, (571) 305-4485
129. Mr. Joseph Yun, Principal Deputy Assistant Secretary, Bureau of East Asian Affairs, Department of State, Washington DC 20520, POC: Mr. John Blanck, (202) 647-7246

Several of these witnesses may become unnecessary depending on the outcome of subsequent Court rulings. The prosecution may add witnesses to this list, depending on the outcome of subsequent Court rulings, to include those relating to Military Rule of Evidence (MRE) 505 and any witnesses relating thereto. The prosecution may replace witnesses on this list, should it become necessary due to a Permanent Change of Station, job relocation, change in job position, or change in level of security clearance of a listed witness.

The prosecution acknowledges an ongoing obligation to provide the defense prompt notice of any other potential witnesses that come to its attention and will adhere to the local rules. The prosecution will communicate its final witness list according to Rule 2.1.8 of the Rules of Practice before Army Courts-Martial (2012) and the Court's order.

If the defense intends to produce a witness who is listed above, the defense must provide a separate, appropriate request for that witness in accordance with Rule for Courts-Martial (RCM) 703 and the standard articulated in United States v. Rockwood, 52 M.J. 98, 105 (1999) that a witness request include a "synopsis of expected testimony," not merely a list of topics to

be covered. If necessary for a particular witness employed by the United States Government, the defense shall also comply with 5 U.S.C. § 301 and Touhy v. Ragen, 340 U.S. 462 (1951).



ASHDEN FEIN
MAJ, JA
Trial Counsel

Enclosure
Classified Supplement to Witness List

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 22 June 2012.



ASHDEN FEIN
MAJ, JA
Trial Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

Prosecution Motion

for Modification of Court Order:
Government Motion: Protective Order(s)
dated 24 April 2012

22 June 2012

RELIEF SOUGHT

The prosecution respectfully requests that the Court modify its existing Order relating to the defense's public release of filings, dated 24 April 2012, three-fold: (1) to authorize the defense to publish their pleadings without the Government reviewing such pleadings; (2) prior to publication of subsequent pleadings, to require the defense to certify to the Court that all such Court filings or proposed filings for which the defense proposes to publicly release do not contain unredacted information subject to an existing protective order; and (3) to order the defense to redact an individual's job title or position, if that individual is not a party to the trial and only one individual holds that job title or position.

BURDEN OF PERSUASION AND BURDEN OF PROOF

The burden of proof on any factual issue the resolution of which is necessary to decide a motion shall be by preponderance of the evidence. RCM 905(c)(1). The burden of persuasion on any factual issue the resolution of which is necessary to decide a motion shall be on the moving party. RCM 905(c)(2).

FACTS

On 24 April 2012, the Court ordered the defense to notify the prosecution of each filing intended for public release and to provide the prosecution with the original filing and the redacted filing intended for public release. See Appellate Exhibit (AE) LXVII. The defense is required to provide this notice to the prosecution by the scheduled filing date for motions, responses, or replies. See id.

The Court ordered the prosecution to address each filing individually and identify, with particularity, each portion of the filing to which the prosecution objects to public release and the legal basis for each objection to public release. The prosecution is required to provide the Court with this information as follows: (1) by the scheduled filing date for responses for defense motions (i.e., two weeks); (2) by the scheduled filing date for replies for defense responses (i.e., five days); and (3) three days after filing of defense replies. See id.

The Court further ordered that personal identifying information will be redacted from all defense filings publicly released. The Court ordered the defense to reference any person who is not a party to the trial by initials of first and last name. See id.

Since 24 April 2012, the defense has submitted filings outside the schedule detailed by the existing case calendar. See, e.g., AE LXXXXIX, AE CI, AE CVI, AE CX, AE CXVI, AE CXX, AE CXXI. Further, the defense has submitted filings that reference individuals who are not parties to the trial by their job title or position, even though there is only one person who holds that particular job title or position. See, e.g., AE CI, AE CXIX.

WITNESSES/EVIDENCE

The prosecution does not request any witnesses or evidence be produced for this motion. The prosecution requests that the Court consider the Enclosures and Appellate Exhibits referenced herein.

LEGAL AUTHORITY AND ARGUMENT

The prosecution respectfully requests that the Court modify its existing Order relating to the defense's public release of filings, dated 24 April 2012, three-fold: (1) to authorize the defense to publish their pleadings without the Government reviewing such pleadings; (2) prior to publication of subsequent pleadings, to require the defense to certify to the Court that all such Court filings or proposed filings for which the defense proposes to publicly release do not contain unredacted information subject to an existing protective order; and (3) to order the defense to redact an individual's job title or position, if that individual is not a party to the trial and only one individual holds that job title or position.

I: THE PROSECUTION REQUESTS THAT THE DEFENSE BE ALLOWED TO PUBLISH SUBSEQUENT COURT FILINGS OR PROPOSED FILINGS UPON CERTIFYING WITH THE COURT THAT THOSE FILINGS DO NOT CONTAIN UNREDACTED INFORMATION SUBJECT TO AN EXISTING PROTECTIVE ORDER.

The prosecution requests that the Court allow the defense to publish subsequent court filings or proposed filings upon certifying with the Court that such filings do not contain any unredacted protected information. Such a result will enable the defense to more expeditiously publish its filings and minimize any administrative burden on the United States Government from future untimely defense filings, without overly burdening the defense.

Since the applicable Court Order on 24 April 2012, the defense has submitted filings outside the schedule detailed by the existing case calendar, requiring the prosecution and the proper agencies, without notice, to coordinate the approval of such unexpected filings.¹ See, e.g., AE LXXXXIX, AE CI, AE CVI, AE CX, AE CXVI, AE CXX, AE CXXI. The Order did not contemplate such a result. Requiring the prosecution to review defense filings submitted

¹ Given the number of agencies involved, reviewing the defense filings requires the prosecution to identify the referenced agencies, submit such filings to those agencies, and coordinate with the proper representatives for approval or necessary redactions. The timeline set forth in the existing Order is consistent with the time necessary to accomplish this task, which is based on the Court's Scheduling Order and does not contemplate off-schedule filings.

outside the scheduled case calendar is overly burdensome for the prosecution and the United States Government as a whole. For the prosecution, such a requirement disrupts its preparation for upcoming Article 39(a) sessions and its continued effort to ensure the accused receives a fair and speedy trial. For the United States Government organizations and agencies, such a requirement disrupts on-going operations and ultimately stalls its support to the court-martial process relating to pretrial and trial matters, including obtaining information and requisite approvals in discovery.

Requiring the defense to certify that its subsequent filings do not contain any unredacted information subject to an existing protective order is not overly burdensome for the defense. Under the present Order, the defense is already required to review the material and redact the information that is protected. Under this proposed modification, the only additional step is for the defense to sign and acknowledge that they have not violated any protective order prior to publically releasing the pleadings. Should any pleading contain protected information, the defense shall properly redact this information prior to public release.

For the above reasons, the prosecution requests that the Court order the defense to certify that subsequent Court filings and proposed filings for which the defense proposes to publicly release do not contain any unredacted information subject to an existing protective order. The prosecution requests that this certification be signed by at least one defense counsel. See Enclosure 1.

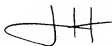
II: ORDERING THE DEFENSE TO REDACT AN INDIVIDUAL'S JOB TITLE OR POSITION, IF THAT INDIVIDUAL IS NOT A PARTY TO THE TRIAL AND ONLY ONE INDIVIDUAL HOLDS THAT JOB TITLE OR POSITION, IS CONSISTENT WITH THE COURT'S PRIOR ORDER.

The existing Court Order states that all persons who are not parties to the trial shall be referenced by initials of first and last name in any defense filing publicly released to protect the safety of potential witnesses. See AE LXVII. Since that Order, the defense has submitted filings that reference individuals who are not parties to the trial by their job title or position, even though there is only one person who holds that particular job title or position. See, e.g., AE CI, AE CXIX. Consistent with the Court's intent to protect the safety of potential witnesses, the prosecution requests that the Court order the defense to redact an individual's job title or position, if that individual is not a party to the trial and only one individual holds that job title or position. Identifying individuals by their job title or position, when only one person holds that job title or position, conflicts with the spirit of the Court's Order and does not protect the safety of those individuals.

CONCLUSION

The prosecution respectfully requests that the Court modify its existing Order relating to the defense's public release of filings, dated 24 April 2012, three-fold: (1) to authorize the defense to publish their pleadings without the Government reviewing such pleadings; (2) prior to publication of subsequent pleadings, to require the defense to certify to the Court that all such Court filings or proposed filings for which the defense proposes to publicly release do not

contain unredacted information subject to an existing protective order; and (3) to order the defense to redact an individual's job title or position, if that individual is not a party to the trial and only one individual holds that job title or position.

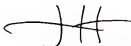


J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

2 Enclosures

1. Certification Sample
2. Draft Order

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 22 June 2012.



J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

) Prosecution Motion
)
)
) for Modification of Court Order:
) Government Motion: Protective Order(s)
) dated 24 April 2012

) Enclosure 1

) 22 June 2012

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Certification of
Defense Court Filings or
Proposed Filings for
Public Disclosure

I. I hereby certify that I have reviewed the Defense Court filing(s) or proposed filing(s) listed in paragraph 3 for information subject to an existing protective order, including but not limited to the following:

a. Appellate Exhibit XXXII;

b. Protective Order for Secretary of the Army AR 15-6 Investigation dated 22 June 2011;

c. Protective Order for Law Enforcement Sensitive Information and Other Sensitive Information dated 22 June 2011, which also incorporates the following federal protective and disclosure orders: 10SW 576, 10SW652, 11EC55, 11EC56, 11EC131, 11MAG841, 11SW47, 11SW89, 11SW94, 10-M-1108, 10SW396, 10SW464, 10GJ3793-11EC1, 10GJ3793-11EC9, 10-330-M-01, 10GJ3793-11EC3, 10GJ3793-RNK, and 10GJ3793-Grand Jury 10-1, 10-2, 10-3, 10-4, 11-1, 11-2, and 11-3.

2. I hereby certify that the Defense Court filing(s) or proposed filing(s) listed in paragraph 3 do(es) not contain any unredacted information subject to an existing protective order. Any information subject to an existing protective order has been properly redacted prior to public disclosure.

3. The Defense Court filing(s) or proposed filing(s) for which I propose to release publicly are as follows:

a. Filing #1;

b. Filing #2; and

c. Filing #3.

SIGNATURE: _____

DATE: _____

NAME: _____

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Prosecution Motion

for Modification of Court Order:
Government Motion: Protective Order(s)
dated 24 April 2012

Enclosure 2

22 June 2012

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)
) **ORDER:**
) **GOVERNMENT MOTION FOR**
) **MODIFICATION OF COURT ORDER:**
) **GOVERNMENT MOTION:**
) **PROTECTIVE ORDER(S)**
) **DATED 24 APRIL 2012**
) **DATED: _____**

1. This Order applies when the Defense intends to release publicly Defense Court filings or proposed filings.
2. A pleading is "filed" with the Court when it is identified as an exhibit on the record at an Article 39(a) session. Pleadings served on the opposing party that have not been identified on the record at an Article 39(a) session are "proposed filings."
3. This Order is issued IAW MRE 505(g) and (h), MRE 506(g) and (h), RCM 701(g) and RCM 806(d), and *Seattle Times v. Rhinehart*, 104 S.Ct. 2199 (1984). The Court finds this Order necessary under the above authorities. The Government has provided the Defense both classified information and government information subject to protective order under MRE 505(g)(1) and MRE 506(g). This Court has issued a protective order for classified information provided to the Defense in discovery. The Defense accepted such discovery and agreed to comply with the protective orders. There have been two classified information spillage incidents to date in this case.
4. This Order supplements the Order issued by the Court on 24 April 2012.

ORDER:

1. The Defense shall review all subsequent Court filings or proposed filings for which the Defense proposes to release publicly for information subject to existing protective orders. The Defense shall redact any such protected information.
2. The Defense shall certify to the Court that such Court filings or proposed filings do not contain any unredacted information subject to an existing protective order. The certification shall state that the Court filings or proposed filings do not contain any information subject to an existing protective order or, in the alternative, that any such information has been properly redacted. The certification shall be signed by at least one defense counsel.
3. To protect the safety of potential witnesses, all persons who are not parties to the trial shall be referenced only by initials of first and last name in any Defense filing publicly released, and not by job title or position, to include listing their job title or position.

So **ORDERED**: this ____ day of _____, 2012.

DENISE R. LIND
COL. JA
Chief Judge, 1st Judicial Circuit

UNITED STATES

 γ_1

DATED: 21 June 2012

APPELLATE EXHIBIT CCLXIV (164)
Page _____ of Page(s)

During the 6 June 2012 hearing, the Court asked the Government if it intended to introduce *any evidence* of actual damage on the merits. The Government responded “No, Your Honor. None.” See Audio Recording of 6 June 2012 Article 39(a). The Government then stated,

But, Your Honor, may I clarify from the perspective of damage assessments then no. But, depending on the definition of damage, we do have to prove prejudicial to good order and discipline and service discrediting. So, it could be conceived of, of immediate damage on the unit, or the perception of the Army or the unit. That could be, that could fall under the umbrella of damage. So for our Clause 1-2 of Article 134 – what would be normally in any other court-martial then, yes. But not, damage from damage assessments that would go to actual harm of national security. We will definitely include that in our brief.

Id.

EVIDENCE

5. The Defense does not request any witnesses be produced for this motion. The Defense requests that this Court consider the following evidence in support of this motion:

- a) Appellate Exhibits LXIV and LXV;
 - b) Audio Recording of 6 June 2012 Article 39(a);
 - c) Attachment A (*WikiLeaks Website Publishes Classified Military Documents from Iraq*, CNN, Oct. 22, 2010);
 - d) Attachment B (*Gates, Mullen Blast WikiLeaks for Disclosures*, Fox News, Jul. 29, 2010);
 - e) Attachment C (Charlie Savage, *Gates Assails WikiLeaks Over Release of Reports*, N.Y. Times, Jul. 30, 2010);
 - f) Attachment D (Adam Levine, *Gates: Leaked Documents Don't Reveal Key Intel, But Risks Remain*, CNN, Oct. 16, 2010);
 - g) Attachment E (*WikiLeaks Iraq War Documents: The Key Issues*, BBC News, Oct. 25, 2010);
 - h) Attachment F (*Are Risks from WikiLeaks Overstated by Government?*, Associated Press, Aug. 17, 2010);
 - i) Attachment G (Nancy A. Youssef, *U.S. Officials: New WikiLeaks Release Will do Most Harm Yet*, McClatchy Tribune News Service, Nov. 27, 2010);
 - j) Attachment H (George Packer, *The Right to Secrecy*, New Yorker, Nov. 29, 2010);
 - k) Attachment I (*Secretary of State Clinton Contacts countries Ahead of WikiLeaks Release*, Seattle Times, Nov. 27 2010);
 - l) Attachment J (*Clinton: WikiLeaks Won't Hurt U.S. Diplomacy*, CBS News, Dec. 2, 2010);
- and
- m) Attachment K (*DOD News Briefing with Secretary Gates and Adm. Mullen from the Pentagon*, U.S. Department of Defense, Nov. 30, 2010).

LEGAL AUTHORITY AND ARGUMENT

6. The Defense reasserts its initial arguments for the relevance and admissibility of information from the various damage assessments. *See* Appellate Exhibit LXV. Additionally, the Defense requests that the Court deny the Government's motion to preclude the Defense from mentioning actual damage on the merits since: 1) the Government's request is overbroad; 2) the information from the damage assessments is proper impeachment evidence; 3) the information from the damage assessments is relevant to the charged offenses; and 4) the information from the damage assessments provides a viable defense.

I. The Government's Request is Overbroad

7. The Government requests that the Court preclude the Defense from "raising or eliciting any discussion, reference, or argument, to include the introduction of any documentary or testimonial evidence, related to actual harm or damage from pretrial motions related to the merits portion of the trial and from the merits portion of the trial." Appellate Exhibit LXIV, at 1. It is unclear what exactly the Government is seeking to prevent the Defense from introducing. If the Government is attempting to prevent the Defense from referencing anything that might be contained in any damage assessment during the merits portion of trial, such a request is overbroad and should be denied by this Court.

8. The Government's request fails to draw a distinction between the Defense referencing the fact that a specific damage assessment concluded the charged information caused no harm or minimal harm, and the Defense referencing specific information contained in the damage assessments. The Government's request requires this Court to ignore any possible use of this information, such as impeaching a witness or providing evidence relevant to a charged offense, and simply rule that this information is not relevant until sentencing.

9. The Government fails to provide the Court with any real justification for granting its request at this time. If the Government believes that a particular line of questioning is not relevant, the Government should object at the time the testimony is being elicited. Only when the Court has the benefit of considering the testimony of the specific witness and the evidence introduced by the parties can the Court determine if a particular line of inquiry is relevant. *See United States v. Swenson*, 51 M.J. 522, 526 (A.F. Ct. Crim. App. 1999) ("By deferring his ruling, the military judge often can better assess the relevance and necessity of the evidence.").

10. Due to the overbroad nature of the Government's request and for the reasons discussed below, the Government's motion should be denied in its entirety.

II. The Information from the Damage Assessments is Relevant Impeachment Evidence

A. The General Nature of the Information from the Damage Assessments

11. The Government has provided notice of the following damage assessments:¹

- a) Department of State damage assessment;
- b) DIA/IRTF damage assessment;
- c) ONCIX damage assessment;
- d) Department of Homeland Security damage assessment;²
- e) FBI Impact Statement;
- f) Any damage assessment by one of the 63 agencies; and
- g) CIA damage assessment.

The Defense has been given an opportunity to review the damage assessments from the Department of State, the DIA/IRTF, the Department of Homeland Security and 25 of 63 governmental agencies that conducted a review for ODNI/ONCIX.

12. Based upon a review of the provided damage assessments, it is clear that the information within the damage assessments is favorable for the Defense. The damage assessments so far contain at least the following information:

a) Factual Assertions: The assessments provide specific factual assertions. By way of example, a factual statement could be “no sources were compromised because all sources were referred to by initials, not names.”

b) Speculative Statements: The assessments also contain qualified statements concerning possible harm from the release of the charged information. Again, by way of example, a speculative statement could be “if X happens, then it could cause harm to our efforts to achieve a certain outcome.”

B. Damage Assessments Can be Used to Impeach Witnesses Who Testify that the Charged Information “Could” Cause Damage

13. Factual assertions or speculative statements regarding the damage caused by the alleged leaks (or, more accurately, the absence of damage) are relevant for the impeachment of Government witnesses who claim that the leaks “could” cause damage. The Government, however, argues that the use of a damage assessment to impeach an Original Classification Authority (OCA) who prepared a classification review would be improper. *See* Appellate Exhibit LXIV, at 3. The Government fails to provide any justification for its position. Why is it improper to use actual *ex post* knowledge (whether derived from a damage assessment or not) to challenge the reasonableness or appropriateness of the *ex ante* classification decision which the Government relies on to show the documents could cause damage? If a doctor, for instance, were called to the stand to testify that a certain chemical “could” cause cancer and the doctor’s

¹ The Government has not yet provided access to the damage assessments from ONCIX, the FBI, CIA, or 38 of the 63 agencies that completed a review for ODNI/ONCIX.

² The Government provided Defense with notification of the existence of the Department of Homeland Security damage assessment for the first time on 8 June 2012. The Government did not indicate when it first learned of the damage assessment or why it had not provided notice to the Court or the Defense of its existence. The Government simply stated that 8 June 2012 was the first time that they were authorized to provide the damage assessment to the Defense.

own hospital or the FDA had published a subsequent report saying that a link had not been established between the chemical and cancer, why could the Defense not use that subsequent knowledge to impeach the witness's testimony that the chemical "could" cause cancer?

14. An OCA witness is not immune from impeachment any more so than any other witness who takes the stand. M.R.E. 607 ("The credibility of a witness may be attacked by any party[.];"); M.R.E. 608 (once a witness testifies, his or her credibility becomes an issue). An OCA's testimony regarding whether certain information could cause damage to the United States or aid any foreign nation is simply that individual witness's opinion. An OCA's opinion is not sacrosanct. *United States v. Diaz*, 69 M.J. 127, 133 (C.A.A.F. 2010) (holding that classification alone is not determinative on the issue of whether information could cause damage to the United States under 18 U.S.C. Section 793). An OCA does not get special treatment, nor is he exempt from cross-examination simply because he is an OCA.

15. Accordingly, the Defense should be able to probe the basis of the OCA's testimony that the information could cause damage by using either factual assertions or speculative statements from the various damage assessments. See *United States v. Israel*, 60 M.J. 485, 486 (C.A.A.F. 2005) ("A defendant's right under the Sixth Amendment to cross-examine witnesses is violated if the military judge precludes a defendant from exploring an entire relevant area of cross-examination." (citing *United States v. Gray*, 40 M.J. 77, 81 (C.M.A. 1994))).

16. For instance, suppose that a damage assessment revealed that Afghani sources were not compromised in the alleged leaks because the sources were referred to in the leaked SIGACTS by initials and not by name. If a Government witness testifies that the information could cause damage, the Defense should be able to information from the damage assessment to question the witness about whether, in making the determination that the information could cause damage, he knew that the sources were referred to by initials. If the witness did not know this, the Defense could probe whether this new information (learned from the damage assessment) would change the witness's view that the information could cause damage. While the Government would neatly have the Court separate the OCA classification reviews from the OCA damage assessments, the analysis is not that tidy. Evidence from the latter is directly relevant to the former and can be used to impeach a witness's credibility.

17. Similarly, suppose that the damage assessment conducted one or two years after the alleged leaks concluded that the released information "could" affect the mission in Afghanistan (not that it "did" affect the mission in Afghanistan). The Defense should be permitted to question a Government witness on the fact that, after a significant period of time had elapsed, the most that a damage assessment was able to conclude was that the information "could" affect the mission in Afghanistan. This would be used to establish that the witness' conclusion that the leaks "could" cause damage is remote and speculative, and thus should not be given weight by the members. The damage or injury that is contemplated under 18 U.S.C. Section 793 cannot be too remote or fanciful, or there is a risk that the section will be converted into a strict liability offense. Anything "could" happen – the world "could" end tomorrow; Kim Kardashian "could" be elected president of the United States of America; I "could" win the lottery. These are not the types of "could" that 18 U.S.C. Section 793 contemplates. Therefore, the Defense should be able to probe whether the witness's testimony that the information could cause damage to the United

States is remote, speculative, far-fetched and fanciful by examining such witnesses on the fact that two years after the alleged leaks, the conclusion is still merely that the information “could” cause damage – not that it “did” cause damage. See *United States v. Johnson*, 30 M.J. 53, 57 (C.M.A.1990), *cert. denied*, 498 U.S. 919 (1990) (indicating that in “means likely” cases, the probability of harm “must at least be more than merely a fanciful, speculative, or remote possibility.”).

18. This Court should not limit the ability of the Defense to examine any OCA or other Government witnesses concerning the factual assertions and speculative statements in the damage assessments since this evidence could undermine the witnesses’ conclusions that the charged information “could” cause harm. See *United States v. Bahr*, 33 M.J. 228 (C.M.A. 1991) (holding military judge’s ruling was an evidentiary and constitutional error by limiting defense in their ability to cross examine the prosecutrix); see also *United States v. Moss*, 63 M.J. 233 (2006) (holding that exclusion of evidence of bias under Rule 608(c) raises issues regarding an accused’s Sixth Amendment right to confrontation if the military judge precludes an accused from exploring an entire relevant area of cross-examination). Unfortunately, the Government seeks to put blinders on the members, the Defense and the witnesses in order to have the “could” analysis take place in an absolute vacuum.

19. If PFC Manning is not permitted to question an OCA or other Government witnesses regarding the factual statements and speculative assertions in the damage assessments, his Sixth Amendment right to confrontation will be violated. Without the ability to undercut the assertions of the OCA or other Government witnesses with the Government’s own conclusions regarding the fact that the charged information did little if any damage, the members will undoubtedly defer to the expertise of the OCA when he testifies the information could cause damage. However, with the benefit of the information from the damage assessments, the members would receive a significantly different impression of an OCA’s credibility when he testifies that the information could cause damage. See *United States v. Collier*, 67 M.J. 347, 352 (C.A.A.F. 2009) (Whether a limitation on the presentation of evidence of bias constitutes a Sixth Amendment violation is “whether ‘[a] reasonable jury might have received a significantly different impression of [the witness’s] credibility had [defense counsel] been permitted to pursue his proposed line of cross-examination.’”). Thus, PFC Manning must be allowed to explore this legally and logically relevant area of inquiry.

C. Damage Assessments Can Be Used to Show Bias of Government Witnesses

20. The Defense believes that any OCA or Government witness who testifies regarding the charged information has an inherent motive to overstate whether the charged information “could” cause harm. The motive to misrepresent by the OCA or other Government witness is due to either anger or embarrassment from the release of the charged information, and/or a desire to support the previous exaggerations by governmental officials concerning the nature or risk or the level of harm due to the charged information being made public. See M.R.E. 608(c) (stating “evidence of bias, prejudice, or any motive to misrepresent may be shown to impeach the witness either by examination of the witness or by evidence otherwise adduced.”).

It is important to recall the Government's initial reaction to the release of the charged information in this case. Then-Pentagon Press Secretary Geoff Morrell stated that:

This is all classified secret information never designed to be exposed to the public. Our greatest fear is that it puts our troops in even greater danger than they inherently are on the battlefields. That it will expose tactics, techniques and procedures – how they operate on the battlefield, how they respond under attack, the capabilities of our equipment . . . how we cultivate sources [and] how we work with Iraqis

Now you will have virtually half a million classified secret documents in the public domain which our enemies clearly intend to use against us That can endanger the lives of American forces, not just in Iraq and Afghanistan, but around the world.

See Attachment A (*WikiLeaks Website Publishes Classified Military Documents from Iraq*, CNN, Oct. 22, 2010, available at <http://edition.cnn.com/2010/US/10/22/wikileaks.iraq/>.) In addition to Mr. Morrell's statements, then-Chairman of the Joint Chiefs of Staff Admiral Mike Mullen stated, "Mr. Assange can say whatever he likes about the greater good he thinks he and his source are doing. But the truth is they might already have on their hands the blood of some young soldier or that of an Afghan family." See Attachment B (*Gates, Mullen Blast WikiLeaks for Disclosures*, Fox News, Jul. 29, 2010, available at <http://www.foxnews.com/politics/2010/07/29/pentagon-wikileaks-blood-hands/>). Likewise Defense Secretary Robert Gates stated in July of 2010 that WikiLeaks would have "potentially dramatic and grievously harmful consequences." See Attachment C (Charlie Savage, *Gates Assails WikiLeaks Over Release of Reports*, N.Y. Times, Jul. 30, 2010, available at <http://www.nytimes.com/2010/07/30/world/asia/30wiki.html>).

21. In spite of the above criticism and conjecture, within a few months the Department of Defense concluded that "the online leak . . . did not disclose any sensitive intelligence sources or methods." See Attachment D (Adam Levine, *Gates: Leaked Documents Don't Reveal Key Intel, But Risks Remain*, CNN, Oct. 16, 2010, available at http://articles.cnn.com/2010-10-16/us/wikileaks.assessment_1_julian-assange-wikileaks-documents?_s=PM:US). Instead, according to Mr. Morrell, the reports consisted primarily of "initial, raw observations by tactical units . . . [which are] essentially snapshots of events, both tragic and mundane." See Attachment E (*WikiLeaks Iraq War Documents: The Key Issues*, BBC News, Oct. 25, 2010, available at <http://www.bbc.co.uk/news/world-us-canada-11617892>). Given the nature of these documents, it was acknowledged that the government knows of no case where anyone in Afghanistan has been harmed because their name was in the leaked documents. See Attachment F (*Are Risks from WikiLeaks Overstated by Government?*, Associated Press, Aug. 17, 2010, available at http://www.salon.com/2010/08/17/wikileaks_risks_overstated/).

22. Likewise, when WikiLeaks announced its intent to release diplomatic cables, the response by the Government was that the leak of these documents would be far more damaging than the first two leaks combined. See Attachment G (Nancy A. Youssef, *U.S. Officials: New WikiLeaks Release Will do Most Harm Yet*, McClatchy Tribune News Service, Nov. 27, 2010, available at

<http://www.mcclatchydc.com/2010/11/27/104388/us-officials-new-wikileaks-release.html>). The government stated that documents could drastically alter U.S. relations with top allies and reveal embarrassing secrets about U.S. foreign policy. *Id.* Government representatives, including Secretary Clinton, asserted that internal communications between U.S. diplomats and the State Department would be less forthright for fear of later exposure, and foreign sources would be less likely to disclose information or share opinions with American diplomats for fear that the U.S. would be unable to protect their statements and identities from disclosure. See Attachment H (George Packer, *The Right to Secrecy*, New Yorker, Nov. 29, 2010, available at <http://www.newyorker.com/online/blogs/georgepacker/2010/11/the-right-to-secrecy.html>; James P. Rubin, *The Irony of WikiLeaks*, New Republic, Dec. 1, 2010, available at <http://www.nnr.com/article/politics/79531/the-irony-wikileaks-american-diplomacy-hard-left>). In an apparent effort to minimize the damage, Secretary of State Hillary Clinton embarked on a global tour to discuss the issue with leaders in various countries. Then-Department of State spokesperson PJ Crowley stated that the release could be “harmful to the United States and our interests and . . . create tension in relationships between our diplomats and our friends around the world.” See Attachment I (*Secretary of State Clinton Contacts countries Ahead of WikiLeaks Release*, Seattle Times, Nov. 27 2010, available at http://seattletimes.nwsource.com/html/nationworld/2013540252_wikileaks28.html?syndication=rss).

23. Again, within a short period of time the Government started to retreat from its dire predictions that the sky was falling. Secretary Clinton downplayed her concerns surrounding the cables after she attended an Organization for Security and Cooperation in Europe meeting where she spoke with foreign leaders who assured her that diplomatic relations would continue as before. See Attachment J (*Clinton: WikiLeaks Won't Hurt U.S. Diplomacy*, CBS News, Dec. 2, 2010, available at <http://www.cbsnews.com/stories/2010/12/01/world/main7105891.shtml> (quoting Secretary Clinton as saying that at the OSCE meeting, “I have not . . . had any concerns expressed about whether any nation will not continue to work with and discuss matters of importance to us both going forward”)). Secretary Gates also confidently declared that the releases would have little effect on diplomatic relations:

But let me – let me just offer some perspective as somebody who’s been at this a long time. Every other government in the world knows the United States government leaks like a sieve, and it has for a long time. And I dragged this up the other day when I was looking at some of these prospective releases. And this is a quote from John Adams: ‘How can a government go on, publishing all of their negotiations with foreign nations, I know not. To me, it appears as dangerous and pernicious as it is novel.’ When we went to real congressional oversight of intelligence in the mid-’70s, there was a broad view that no other foreign intelligence service would ever share information with us again if we were going to share it all with the Congress. Those fears all proved unfounded.

Now, I’ve heard the impact of these releases on our foreign policy described as a meltdown, as a game-changer, and so on. I think – I think those descriptions are fairly significantly overwrought. The fact is, governments deal with the United States because it’s in their interest, not because they like us, not because they trust us, and not because they believe we can keep secrets. Many governments – some

governments deal with us because they fear us, some because they respect us, most because they need us. We are still essentially, as has been said before, the indispensable nation. So other nations will continue to deal with us. They will continue to work with us. We will continue to share sensitive information with one another. Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest.

See Attachment K (*DOD News Briefing with Secretary Gates and Adm. Mullen from the Pentagon*, U.S. Department of Defense, Nov. 30, 2010, available at <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4728> (transcript of press conference)). Secretary Gates also stated "...I thin, in all of these releases, whether it's Afghanistan, Iraq, or the releases this week [diplomatic cables], is the lack of any significant difference between what the U.S. government says publicly and what they things show privately...." *Id.*

24. The Defense has now had the benefit of reviewing the Information Review Task Force's damage assessment and the Department of State's August 2011³ draft damage assessment. The damage assessments underscore what the Defense has suspected all along in regards to the speculative damage supposedly caused by the alleged leaks.

25. The Defense should be entitled to use the draft damage assessments to impeach any witness from the Department of Defense, Department of State, or any other governmental agency. Based on the over-reaction of government officials to the leaks (described above), witnesses will have a motivation to lie or at least overstate whether the leaks "could" cause damage.

26. The impeachment rules are required to be read to allow liberal admission of bias-type evidence. See *United States v. Hunter*, 21 M.J. 240 (C.M.A.), cert. denied, 476 U.S. 1142 (1986); see also *United States v. George*, 40 M.J. 540 (A.C.M.R. 1994) (military judge improperly restricted defense cross-examination of government toxicology expert. Questions about the expert's salary and possible sources of contamination of the urine sample were relevant to explore bias); *United States v. Aycock*, 39 M.J. 727 (N.M.C.M.R. 1993) (military judge abused his discretion and committed prejudicial error in excluding extrinsic evidence of a government witness's bias and motive to testify falsely). The Defense should not be arbitrarily limited in exploring an entire relevant area of impeachment (i.e. bias) simply because the Government does not wish for panel members to know about America's worst-kept secret – that the alleged leaks did little to no harm to national security. It is axiomatic that it is the role of the members to determine the credibility of any witness. Accordingly, bias evidence, if logically and legally relevant, is properly presented to the members.

III. The Information from the Damage Assessment is Relevant to Charged Offenses

A. The Lack of Harm Goes to An Element of the Charged Offenses

³ The Department of State did not even believe it was worthwhile to update its damage assessment after the entire diplomatic database was released in unredacted form in September of 2011. See Ms. Catherine Brown's testimony (audio recording of 7 June 2012 Article 39(a)). The fact the Department of State did not embark on an effort to verify possible damage should speak volumes regarding the real likelihood of any such damage.

27. The Government states that it will not seek to introduce any evidence of actual damage on the merits. *See* Audio Recording of 6 June 2012 Article 39(a) (transcript of colloquy provided in factual section of brief above). However, in the same breath, the Government says that damage may be relevant to the Clause 1 and 2 lesser included offense (LIO) of the various offenses. *Id.* So it appears that the Government would like to have its cake and eat it too. It would like to prevent the Defense from referencing the absence of harm, but would like to reserve its right to argue that harm was caused for the limited purpose of the Clause 1 and 2 elements of the charged offenses.

28. The absence of harm is relevant to whether PFC Manning's conduct was prejudicial to good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces. The relevance of this information is not controlled by how the Government attempts to prove the Clause 1 and 2 elements of the charged offenses. In the same manner the Government may seek to use this information to prove conduct that would satisfy the Clause 1 and 2 elements of the charged offenses, the Defense should be entitled to use the lack of damage to prove that the charged conduct was not prejudicial to good order and discipline or service discrediting. If the charged information caused no damage and, in fact, did overall good, the conduct can hardly be said to rise to the level of conduct that is prejudicial to good order and discipline or service discrediting.

29. Not only is damage or the lack of damage relevant to the Clause 1 and 2 elements of the charged offenses, but it is also relevant to the following:

a) 18 U.S.C. Section 793 and the 18 U.S.C. Section 1030 offenses: The absence of harm is relevant to whether PFC Manning had reason to know that the information released could be used to the injury of the United States or to the advantage of a foreign nation. *See* Charge Sheet.

b) 18 U.S.C. Section 641: The absence of harm is relevant to whether there was a substantial interference with the Government possession and thus a conversion of the information. *Id.*

c) Specification I of Charge II. The absence of harm is relevant to whether PFC Manning acted recklessly or wantonly, an element of the charged offense. *Id.*

18 U.S.C. Section 793(e) and 1030(a)(1) Offenses

30. In order to prove PFC Manning is guilty of either the Section 793(e) or 1030(a)(1) offenses, the Government must prove that PFC Manning knew or had a reason to believe that the charged information could be used to the injury of the United States or to the advantage of any foreign nation. "Reason to believe" means that PFC Manning knew facts from which he concluded or reasonably should have concluded that the charged information could be used for the prohibited purposes. *Gorin v. United States*, 312 U.S. 19 (1941); *United States v. Truong Dinh Hung*, 629 F.2d 908, 919 (4th Cir. 1980); *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979). In considering whether or not PFC Manning had reason to believe that the charged information could be used to the injury of the United States, or to the advantage of any foreign nation, a panel member should be entitled to consider whether harm actually occurred, so as to test the reasonableness of PFC Manning's belief that this information could not cause damage to the United States.

31. The Government would seek to prevent the panel members from having the benefit of hindsight in determining whether PFC Manning had “reason to believe” the information “could be used to the injury of the United States or the advantage of a foreign nation.” The Government argues that this Court should create a wall between the merits and the sentencing phase regarding this vital information. It is clear that the Government is hoping that the panel members will simply defer to the classification decisions of various OCAs regarding the conclusion that classified information “could” cause harm. Unfortunately for the Government, the Court of Appeals for the Armed Forces (CAAF) has rejected such a simplistic inference by the members. The CAAF has clearly stated that the classification of a document is only probative, and not determinative, of the issue of whether information could cause harm. *United States v. Diaz*, 69 M.J. 127, 133 (C.A.A.F. 2010); *see also United States v. Morison*, 844 F.2d 1057, 1086 (4th Cir. 1988) (“[N]otwithstanding information may have been classified, the government must still be required to prove that it was *in fact* ‘potentially damaging . . . or useful,’ i.e., that the fact of classification is merely probative, not conclusive, on that issue”). Therefore, the panel members should not be denied relevant evidence on this issue.

32. Under *Diaz*, the Government cannot satisfy its burden of showing that the documents could cause damage merely by pointing to their classification.⁴ Instead, the Government must produce some witness testimony or additional evidence to satisfy its burden. The Defense is entitled to challenge this testimony or additional evidence. The Defense should be permitted to argue that, by virtue of his expertise and training, PFC Manning knew which documents and information could be used to the injury of the United States or to the advantage of any foreign nation. PFC Manning had access to a great deal of very sensitive information that, if disclosed, could have caused damage to the United States. By selecting the information that he allegedly did, PFC Manning deliberately chose information that could not cause damage to the United States. The reasonableness of his belief that the information could not cause damage is buttressed by the damage assessments which say that the leaks did not cause damage to the United States. In short, the Defense submits that the damage assessments confirm that PFC Manning did not have “reason to believe” that the information could cause damage to the United States or be used to the advantage of a foreign nation.

33. The Court specifically requested the parties to explore case law on the issue of “what happened” being relevant to “what could happen.” Audio from 6 June 2012 Article 39(a) hearing. Given the lack of case law covering the charged offenses in this regard, the Court suggested that the parties explore the issue in the context of assault with a means likely to produce death or grievous bodily harm. *Id.*; *see generally* Article 128 Para. 54c(4)(a).

34. *United States v. Hudson* provides an excellent example of “what happened” being relevant to “what could happen.” 2000 WL 228777 (N-M. Ct. Crim. App. 2000). In *Hudson*, the court

⁴ The Government cites *Diaz* for a completely unrelated proposition that is not at issue here. *See* Government Motion, at 6. The motion to preclude evidence in *Diaz* was related to intent, not relevance. In *Diaz*, the military judge excluded evidence that the Defense contended would satisfy the heightened *mens rea* requirement in 18 U.S.C. Section 793(e) of “intent to do harm” or “bad faith.” *Id.* at 137. Given that the Court concluded there was no heightened *mens rea* requirement for Section 793(e), the exclusion of the evidence was proper. This ruling does not speak at all to whether it is appropriate to exclude reference to actual harm in this case.

found the evidence to be insufficient to support a conviction for assault with a means likely to produce grievous bodily harm. The court used a two pronged test for its determination “(1) the risk of harm and (2) the magnitude of the harm.” *Id.* at *2 (citing *United States v. Outhier*, 45 M.J. 326, 328 (C.A.A.F. 1996)). The court stated that “the likelihood of death or grievous bodily harm was determined by measuring both prongs, not just the statistical risk of harm.” *Id.*

35. Using the analysis that looked at “what happened” in order to determine “what could happen,” the court held that the evidence fell short. Although the appellant assaulted his wife “by grabbing her with his hands, slamming her against the wall, causing her head to hit the wall, by pulling her across the room by her hair, and by pushing her to the floor causing her to strike a bed and nightstand” the court concluded that this “did not create a high degree of risk to cause grievous bodily harm” (the first prong). *Id.* at *1-2. Similarly, the court concluded that the “magnitude of harm was not great” (the second prong). *Id.* at *2. The court noted that the doctor who examined the wife the following day found only minor injuries and the wife suffered no fractures, dislocations, broken bones, deep cuts, or damage to any internal organs. *Id.* Therefore, the court was not convinced beyond a reasonable doubt of the appellant’s guilt of assault with a means likely to produce grievous bodily harm. *Id.* In concluding that the evidence was factually insufficient to sustain a conviction, the *Hudson* court clearly considered “what happened” in order to inform its decision of “what could happen.”⁵ So too should this Court allow the panel members to consider “what happened” in order to inform its decision of “what could happen.”

36. Similarly, in *United States v. Outhier*, 45 M.J. 326 (C.A.A.F. 1996), the CAAF found the accused’s plea improvident as to aggravated assault with a means likely to produce death or grievous bodily harm. The Court noted that “while it is well-settled that there is no requirement to prove . . . any resultant injury or harm in order to prove aggravated assault, we recognize that these circumstances frequently provide the lynch-pin between a means that is used in a manner “likely” to produce death or grievous bodily harm and one that is not.” *Id.* at 329. The court held that it was “the circumstances [that] define whether the means used were employed in a manner likely to cause grievous bodily harm.” *Id.* After canvassing these circumstances, the court concluded, “Under these circumstances, we cannot hold that the plea provided factual support for the conclusion that appellant’s actions were likely to result in death or grievous bodily harm. *In fact, no harm occurred.*” *Id.* at 330 (emphasis supplied). As is clear, whether harm occurred was a factor considered by the court in coming to its conclusion that the plea was not provident as to the “means likely” offense.

37. In *United States v. Joseph*, 33 M.J. 960 (N-M.C.M.R. 1991), the court stated:

Whether the conduct of the accused charged as an aggravated assault involves a means used in a manner likely to produce death or grievous bodily harm ultimately becomes a question to be determined by the fact finder. The evidence need not establish that death or grievous bodily harm was highly probable or even more likely than not, and no required statistical probability can be found in

⁵ The court held that it was insufficient to prove merely that death or grievous bodily harm was “possible.” Instead, the Court concluded the Government must prove that it was “probable.” *Id.* at *2 (citing *United States v. Weatherspoon*, 49 M.J. 209, 211, (C.A.A.F. 1998)).

decisional law. It is for the fact finder to consider *all* the evidence and determine beyond a reasonable doubt whether the risk of harm meets the general statutory requirement, although the law clearly does require that the risk amount to more than “merely a fanciful, speculative, or remote possibility” of harm.

33 M.J. at 964 (emphasis supplied). Thus, two things are clear from this passage. First, the risk of harm must be more than merely “fanciful, speculative or remote.” *Id.* Second, it is the job of the fact-finder to consider *all* the evidence (including whether harm actually resulted) and determine whether the assault was with a means likely to produce death or grievous bodily injury.

38. As stated above, the Government must prove that the information could cause damage, and more specifically, that the accused had reason to believe that the information could cause damage. The Defense should be entitled to rebut the Government’s proof by showing that the accused did not have reason to believe that the information could cause damage and testing the reasonableness of that belief against the actual damage caused (or, as the Defense would submit, the absence of damage caused). Whether this line of defense is compelling to the members goes to weight, not admissibility of the evidence. Relevant evidence is simply evidence that has “*any tendency* to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.” See M.R.E. 401 (emphasis supplied). The “any tendency” standard is the lowest possible standard for relevancy. *United States v. Schlamer*, 52 M.J. 80 (C.A.A.F. 1999) (holding that M.R.E. 401 is a low standard and the admitted evidence had some tendency to support a fact at issue); see also *United States v. Berry*, 61 M.J. 91 (C.A.A.F. 2005) (discussing any tendency standard being a low standard). If the facts are that the information either did not cause damage or caused minimal damage, this would have at least some tendency to confirm that PFC Manning did not have “reason to believe” that the information could cause damage to the United States or be used to the advantage of a foreign nation. *United States v. Truong Dinh Hung*, 629 F.2d 908, 919 (4th Cir. 1980) (approving jury instruction that “reason to believe” meant that a defendant must be shown to have known facts from which he concluded or reasonably should have concluded that the information could be used for the prohibited purposes). This plainly satisfies the lenient “any tendency” standard for relevancy.

18 U.S.C. Section 641 Offenses

39. In Specifications 4, 6, 8, 12 and 16 of Charge II, PFC Manning is charged with violations of Section 641 under clause 3 of Article 134. See Charge Sheet. Under the charged specifications, the absence of harm is relevant to whether there was a substantial interference with the Government’s property interest and thus a conversion of the information under Section 641.

40. The key requirement of conversion under Section 641 is that an accused must exercise control over the property in such a manner that serious interference with the rights of the owner result. *United States v. Wilson*, 636 F.2d 225 (8th Cir. 1980); *United States v. May*, 625 F.2d 186 (8th Cir. 1980). In determining whether there has been a substantial interference, members must be able to consider any actual harm or the absence of harm from the various damage assessments. Under relevant case law, serious interference is one that prevents the government

from making some other use of the property. *United States v. Kueneman*, 94 F.3d 653 (9th Cir. 1996) (the court reversed appellant's conviction under Section 641 when it determined that the government could not show any harm due to the appellant's conduct); *United States v. Collins*, 56 F.3d 1416, 1421 (D.C. Cir. 1995) (after explaining that a charge of conversion requires *serious interference* with property rights, the court found that the charges related to computer use and storage were not supported where no evidence was offered showing the conduct "prevented [the defendant] or others from performing their official duties"); *United States v. Matzkin*, 14 F.3d 1014, 1020 (4th Cir. 1994) (the court considered the amount of damage to the government in concluding whether the appellant violated §641).

41. Actual damage, or lack thereof, is relevant on the merits as it relates to charges under Section 641. This information would indicate the extent (if any) of "serious interference" with property rights of the Government. In deciding whether the Government has met its burden, the members should be able to consider information from the various damage assessments. Because evidence of actual damage is relevant, the Defense should be allowed to present this evidence to the members.

Specification 1 of Charge II

42. In Specification 1 of Charge II, PFC Manning is charged with wrongfully and wantonly causing United States intelligence to be published on the internet, having knowledge that the intelligence placed on the internet is accessible to the enemy, in violation of Article 134. *See* Charge Sheet. The absence of harm is relevant to whether PFC Manning acted recklessly or wantonly, an element of the charged offense. *Id.* Although the MCM does not define the term "wanton" in the context of disclosure of information, it does define the term in two other contexts. *See* MCM, Part IV, para. 35.c(8) (defining "wanton" for purposes of Article 111); *id.*, Part IV, para. 100a.c(4) (defining "wanton" for purposes of Article 134, offense of "reckless endangerment"). Both definitions provided by the MCM are essentially the same: "'Wanton' includes 'Reckless' but may connote willfulness, or a disregard of probable consequences, and thus describe a more aggravated offense." *Id.*, Part IV, para. 100a.c(4); *see id.*, Part IV, para. 35.c(8) ("'Wanton' includes 'reckless', but in describing the operation or physical control of a vehicle, vessel, or aircraft 'wanton' may, in a proper case, connote willfulness, or a disregard of probable consequences, and thus describe a more aggravated offense.").

43. Thus, "wanton" as used in the clause 3 Article 134 offense will necessarily involve an assessment of whether it was indeed reckless to release the charged information to WikiLeaks or whether PFC Manning disregarded the probable consequences of his actions by engaging in the alleged conduct. As such, the Defense should be entitled to use the factual assertions and speculative statements within the damage assessments, as well as evidence related to the absence of harm, to dispute that PFC Manning's conduct was potentially "wanton" or "wrongful" for the purposes of Specification 1 of Charge II.

IV. The Court Should Not Preclude the Defense From Raising a Viable Defense

44. The Government's effort to preclude the Defense from referencing any information from the various damage assessments is identical to the tactic attempted in *United States v. Drake*. No.

RDB-10-181 (D. Md. Mar. 31, 2011). The government in *Drake* attempted to preclude the defense from referencing certain evidence during the merits. The court expressed an unwillingness to foreclose a potential line of argument, especially given that the court had the inherent power to control the courtroom. The court stated in this respect:

THE COURT: -- but my point is that, to preclude them from going down that path, I think, essentially prevents them from presenting a defense, that we can control the matter of whether or not there is reference to necessity or justification, *and I'm fairly confident I'll be able to control the courtroom to do that.* It's just a matter of where else we go with this motion, and it seems to me they're certainly entitled to get into this.

* * *

THE COURT: As I interpret the Government's motion, or as I intend to interpret it, it doesn't mean that that evidence is -- although the Government seems very concerned with it amounting to a higher calling, necessity, or justification defense, *I'm fairly confident that I can keep this case on track to correct you if you happen to make an inadvertent mistake in that regard,* but you're certainly free to have at that in terms of the intent element, and that's how I see it.

Transcript of Record at M-100, M-103, *United States v. Drake*, No. RDB-10-181 (D. Md. Mar. 31, 2011) (emphasis supplied).

45. PFC Manning should be permitted to prove that he knew which documents and information could not be used to the injury of the United States or to the advantage of any foreign nation. In order to buttress the reasonableness of his belief that the information could not cause damage, this Court should conclude that PFC Manning is entitled to use information and conclusions from the damage assessments.

46. In *United States v. Diaz*, the CAAF held that the military judge erred by preventing the appellant from presenting motive evidence on an Article 133, UCMJ charge. 69 M.J. 127 (C.A.A.F. 2010). The CAAF determined that the evidence could have informed a factfinder's judgment as to whether the appellant's conduct was unbecoming an officer. *Id.* at 136. Similarly, the damage assessment information would inform a factfinder's judgment as to whether PFC Manning's conduct was prejudicial to good order and discipline or service discrediting; could cause damage to the United States or aid any foreign nation; substantially interfere with the government's use of the charged information; or constitute a reckless and wanton disregard for the consequences of his actions.

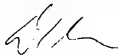
47. PFC Manning had access to a great deal of very sensitive information that, if disclosed, could have caused damage to the United States. By virtue of his expertise and training he should be entitled to assert that he selected information that could not be used to the injury of the United States or to the advantage of any foreign nation. In order to support this viable defense, the Defense must be allowed to challenge the testimony of any Government witness by introducing

factual assertions and speculative statements from the various damage assessments and must be permitted to argue that the leaked information did not cause harm to the United States.

CONCLUSION

48. For the reasons outlined herein, the Defense requests that this Court deny the Government's motion in its entirety. In the alternative, the Defense requests that this Court defer ruling on the motion until the issue is ripe.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. E. Coombs', with a stylized flourish at the end.

DAVID EDWARD COOMBS
Civilian Defense Counsel

ATTACHMENT A

WikiLeaks website publishes classified military documents from Iraq

By the CNN Wire Staff

October 25, 2010 — Updated 1723 GMT (0123 HKT)

CNN.com



Washington (CNN) -- The whistle-blower website WikiLeaks published nearly 400,000 classified military documents from the Iraq war on Friday, calling it the largest classified military leak in history.

The latest round of leaked documents provides a new picture of how many Iraqi civilians have been killed, a

new window on the role that Iran has played in supporting Iraqi militants and many accounts of abuse by Iraqi's army and police, according to The New York Times.

The Times was one of a handful of news organizations that was provided early access to the papers.

According to new documents, the vast majority of slain civilians were killed by other Iraqis.

The U.S. military is notifying Iraqis named in the documents, Pentagon Press Secretary Geoff Morrell told CNN.

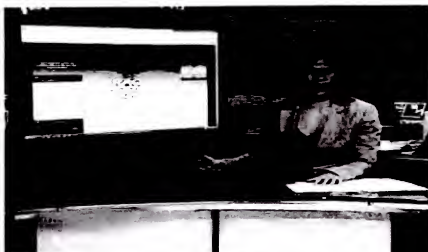
"There are 300 names of Iraqis in here that we think would be particularly endangered by their exposure," he said. "We have passed that information on to U.S. Forces Iraq. They are in the process right now of contacting those Iraqis to try to safeguard them."

The Pentagon had not previously warned Iraqi civilians who have cooperated with the United States that their names may be posted on the Internet.

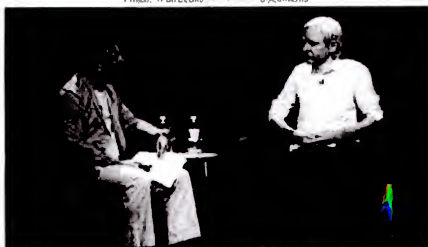
"We don't want to start notifying people and then find out that their names aren't in any of these documents that are released," Col. David Lapan, a top Pentagon spokesman, said earlier Friday. "Why put people through the trouble and the concern for no reason?"

The Pentagon denounced the release, which WikiLeaks said comprised 391,832 reports.

"This is all classified secret information never designed to be exposed to the public," Morrell told CNN Friday. "Our greatest fear is that it puts our troops in even greater danger than they inherently are on these battlefields. That it will expose tactics, techniques and procedures -- how they operate on the battlefield, how they respond under attack, the capabilities of our equipment ... how we cultivate sources (and) how we work with Iraqis."



Video: WikiLeaks releases documents



London: US Secretary of Defense Robert Gates



Video: US Secretary of Defense



classified documents from the war in Afghanistan, Chairman of the Joint Chiefs of Staff Adm. Mike Mullen said WikiLeaks "might already have on their hands the blood of some young soldier or that of an Afghan family."

Morrell echoed that sentiment Friday.

"We know in the aftermath of the Afghan document leak that the Taliban and others spoke publicly, encouraging their members to mine that database -- our intelligence confirmed that fact," he told CNN. "Now you will have virtually half a million classified secret documents in the public domain which our enemies clearly intend to use against us."

"That can endanger the lives of American forces, not just in Iraq and Afghanistan, but around the world," Morrell said.

WikiLeaks has shown a much heavier hand redacting the new round of documents compared to its previous publication of documents.

Editor-in-chief Julian Assange told CNN's Atika Shubert the site was more "vigorous" this time compared to the Afghanistan process.

Read more on WikiLeaks' redaction of information

An initial comparison of a few documents redacted by WikiLeaks to the same documents released by the Department of Defense shows that WikiLeaks removed more information than the Pentagon.

The documents detail Iran's role in supplying Iraqi militia fighters with weapons, including the most lethal type of roadside bomb.

Field reports released Friday assert that Iraqi militants traveled to Iran for training as snipers and in using explosives, according to the Times. Iran's Quds Force urged Iraqi extremists it was working with to kill Iraqi officials, the Times reported.

CNN was offered access to the documents in advance of the release but declined because of conditions that were attached to accepting the material.

According to an analysis by the Guardian, a British newspaper, the documents detail torture, summary executions and war crimes.

U.S. authorities failed to investigate hundreds of reports of abuse, torture, rape and murder by Iraqi police and soldiers, the documents show, according to the Guardian.

The Times said that hundreds of reports of beatings, burnings and lashings suggested that "such treatment was not an exception." Most abuse cases contained in the new batch of leaks appear to have been ultimately ignored, the paper said.

The Times said that military rules require forces to report abuse to Iraqi authorities, but suggested

that there was little follow-up on abuse reports.

The group Iraq Body Count said that the new documents reveal 15,000 previously unknown civilian deaths, raising the group's civilian death toll to 122,000.

"It's the largest single addition to our database since we began it," the anti-war group's co-founder, John Sloboda, told CNN.

WikiLeaks' Assange told CNN in an exclusive interview Friday that the new round of field reports shows "compelling evidence of war crimes" committed by forces of the U.S.-led coalition and the Iraqi government.

The Pentagon's Morrell rebutted that charge.

"We vetted every single one of the documents, word by word, page by page," Morrell told CNN, saying the vetting began in July. "There is nothing in here which would indicate war crimes. If there were, we would have investigated it a long time ago."

A group of 120 Defense Department experts has been poring over hundreds of thousands of "Significant Action Reports" that they expected to be posted to the WikiLeaks website.

In a news release, the group said the documents detail 109,032 deaths in Iraq, encompassing 66,081 civilians, 23,984 insurgents, 15,196 Iraqi government forces and 3,771 coalition forces, according to the classifications used by the U.S. military.

Assange said the documents contained more than 1,000 reports on the torture or abuse of detainees by Iraqi government forces and that he expects that 40 wrongful death lawsuits will be filed as a result of the new leaks.

He dismissed concerns that the publication of the documents could endanger U.S. troops and Iraqi civilians, asserting that the Pentagon "cannot find a single person that has been harmed" due to WikiLeaks' previous release of 76,000 pages of documents related to the U.S.-led war in Afghanistan.

"We strongly condemn the unauthorized disclosure of classified information and will not comment on these leaked documents other than to note that 'significant activities' reports are initial, raw observations by tactical units," the Department of Defense said in a Friday statement. "They are essentially snapshots of events, both tragic and mundane, and do not tell the whole story. That said, the period covered by these reports has been well-chronicled in news stories, books and films and the release of these field reports does not bring new understanding to Iraq's past.

"However, it does expose secret information that could make our troops even more vulnerable to attack in the future," the statement continued. "Just as with the leaked Afghan documents, we know our enemies will mine this information looking for insights into how we operate, cultivate sources, and react in combat situations, even the capability of our equipment. This security breach could very well get our troops and those they are fighting with killed."

Ryan Crocker, former U.S. Ambassador to Iraq, said this week he is concerned for the safety of the Iraqis who may be mentioned.

"What I'd really be worried about in this context, we're not fighting a hot war," Crocker said in remarks at the Center for Strategic and International Studies on Tuesday. "It's not the same set of issues in Afghanistan, although there may be some carryover. I'd really be worried if, as looks to be the case, you have Iraqi political figures named in a context or a connection that can make them politically and physically vulnerable to their adversaries.

"It just has an utterly chilling effect on the willingness of political figures to talk to us, not just in Iraq, anywhere in the world. And I think a hugely irresponsible step on the part of WikiLeaks. Just in a different sense than we saw in Afghanistan, this, too, is going to put lives at risk needlessly and irresponsibly."

CNN's Larry Shaughnessy contributed to this report.



© 2011 Cable News Network. Turner Broadcasting System, Inc. All Rights Reserved.

ATTACHMENT B



Print Close

Gates, Mullen Blast WikiLeaks for Disclosures

Published July 29, 2010 | FoxNews.com

Top Pentagon officials assailed WikiLeaks on Thursday for its release of thousands of pages of leaked documents covering the war in Afghanistan -- at one point even accusing the man behind the whistle-blower website of having "blood... on his hands."

Defense Secretary Robert Gates and Joint Chiefs of Staff Chairman Adm. Mike Mullen issued some of their harshest criticisms yet of the leak, which appeared to include the names of Afghans enlisted as classified U.S. military informants.

WikiLeaks founder Julian Assange has defended the release, but Mullen dismissed his arguments.

"Mr. Assange can say whatever he likes about the greater good he thinks he and his source are doing, but the truth is they might already have on their hands the blood of some young soldier or that of an Afghan family," Mullen said.

Gates said he called FBI Director Robert Mueller seeking assistance in the ongoing investigation into the leak of the documents, though Gates wouldn't comment on reports that the leak was the work of Pvt. Bradley Manning, an Army intelligence analyst already under suspicion in an earlier leak of classified materials to WikiLeaks.

The criminal investigation into the leak could go beyond the military, Gates said, and he did not rule out that Assange could be a target.

"The investigation should go wherever it needs to go," Gates said.

He would not be more specific, waving off questions about whether Assange or media outlets that used the WikiLeaks material could be subjects of the criminal probe. But he noted that he has asked the FBI to help in the investigation "to ensure that it can go wherever it needs to go."

Gates and Mullen called the release of the documents that WikiLeaks calls its "Afghan War Diary" deeply damaging and potentially life-threatening for Afghan informants or others who have taken risks to help the U.S. and NATO war effort.

That's was the most sober assessment of the ramifications of the leak Sunday of raw intelligence reports and other material dating to 2004.

The Army is leading an inquiry inside the Defense Department into who downloaded some 91,000 secret documents and passed the material to WikiLeaks, an online archive that describes itself as a public service organization for whistleblowers, journalists and activists.

The FBI would presumably handle aspects of the investigation that involve civilians outside the Defense Department, and the Justice Department could bring charges in federal court.

Assange agreed Tuesday that the files offered insight into U.S. tactics.

But he said that was none of his concern, and seemed irritated when a questioner in London pressed him on whether he believed there were ever any legitimate national security concerns that would prevent him from publishing a leaked document.

"It is not our role to play sides for states. States have national security concerns, we do not have national security concerns," he said.

Gates said that the Pentagon is tightening rules for handling classified material in war zones as a result of the leak. He did not mention Manning by name, and Pentagon officials caution that Manning may not be the sole target of the Army inquiry.

Manning was stationed at a small post outside Baghdad. If he was the source of the Afghan war logs, he would have been

emassing material he had little if any reason to see.

"If the kind of breach involved in the downloading of these thousands of documents had occurred at a rear headquarters or here in the U.S., there's a very high likelihood we would have detected it," Gates said.

Fox News' Pat Summers and the Associated Press contributed to this report.

 [Print](#)  [Close](#)

URL

<http://www.foxnews.com/http://www.foxnews.com/politics/2010/07/29/pentagon-wikileaks-blood-hands/>

[Home](#) | [Video](#) | [Politics](#) | [U.S.](#) | [Opinion](#) | [Entertainment](#) | [SciTech](#) | [Health](#) | [Travel](#) | [Lifestyle](#) | [World](#) | [Sports](#) | [Weather](#)

[Privacy](#) | [Terms](#)

This material may not be published, broadcast, rewritten, or redistributed. © 2012 FOX News Network, LLC. All rights reserved. All market data delayed 20 minutes.

ATTACHMENT C

Gates Assails WikiLeaks Over Release of Reports

By CHARLIE SAVAGE

Published: July 29, 2010

WASHINGTON — Defense Secretary Robert M. Gates on Thursday denounced the disclosure this week of 75,000 classified documents about the Afghanistan war by the Web site WikiLeaks, asserting that the security breach had endangered lives and damaged the ability of others to trust the United States government to protect their secrets.

Speaking to reporters at the Pentagon, Mr. Gates portrayed the documents as “a mountain of raw data and individual impressions, most several years old” that offered little insight into current policies and events. Still, he said, the disclosures — which includes some identifying information about Afghans who have helped the United States — have “potentially dramatic and grievously harmful consequences.”

“The battlefield consequences of the release of these documents are potentially severe and dangerous for our troops, our allies and Afghan partners, and may well damage our relationships and reputation in that key part of the world,” he said. “Intelligence sources and methods, as well as military tactics, techniques and procedures, will become known to our adversaries.”

The Times has taken care not to publish information that would harm national security interests or disclose anything that was likely to put lives at risk or jeopardize military or antiterrorist operations, withholding any names of operatives in the field and informants cited in the reports. It also has not linked to the archives of raw material.

Mr. Gates said the documents’ disclosure had prompted a rethinking of a trend nearly two decades old, dating from the Persian Gulf war of 1991, of trying to make intelligence information more accessible to troops in combat situations so they can respond rapidly to developments.

“We endeavor to push access to sensitive battlefield information down to where it is most useful — on the front lines — where as a practical matter there are fewer restrictions and controls than at rear headquarters,” he said. “In the wake of this incident, it will be a real

challenge to strike the right balance between security and providing our frontline troops the information they need."

The military has charged an intelligence analyst, Pfc. Bradley Manning, with downloading large amounts of classified information from a computer at a base in Iraq and sending it to WikiLeaks, which operates from servers scattered across multiple countries and solicits "classified, censored or otherwise restricted material of political, diplomatic or ethical significance."

Military officials have said that Army investigators also consider Private Manning a "person of interest" in the investigation into the Web site's most recent disclosures. They said Thursday that he was being moved from Kuwait to Quantico, Va., where he would remain in military confinement as he awaits further judicial steps. WikiLeaks shared the documents with publications in Britain, Germany and the United States, including The New York Times, before posting them this week.

Julian Assange, an Australian computer specialist who founded WikiLeaks, has described the project as a form of journalism that seeks to protect whistle-blowers and enhance democracy by making public information that government officials would rather keep secret.

In a series of media appearances and interviews this week, he has defended the latest release as providing an unvarnished portrait of problems with the war in Afghanistan, while saying that his organization had held back about 15,000 documents for safety reasons.

But at Mr. Gates's news conference on Thursday, the chairman of the Joint Chiefs of Staff, Adm. Mike Mullen, portrayed WikiLeaks as recklessly endangering people in order to satisfy its "need to make a point."

"Mr. Assange can say whatever he likes about the greater good he thinks he and his source are doing, but the truth is they might already have on their hands the blood of some young soldier or that of an Afghan family," Admiral Mullen said.

Mr. Gates said the military was taking steps to protect some Afghans identified in the documents, but he declined to specify them. He also declined to comment about the investigation beyond noting that he had enlisted the Federal Bureau of Investigation to assist Army investigators, a move that is seen as a precursor to potentially charging people who are not uniformed service members.

A person familiar with the investigation has said that Justice Department lawyers are exploring whether Mr. Assange and WikiLeaks could be charged with inducing, or conspiring in, violations of the Espionage Act, a 1917 law that prohibits the unauthorized disclosure of national security information.

ATTACHMENT D

U.S.

Ads by Google

Risk Management Courses

Stanford's Strategic Decisions and Risk Management Certificate.

Stanford.edu

Prudential Can Help

Together, let's tackle our biggest financial challenges. Learn more.

Prudential.com/bringyourchallenges

Related Articles »Julian Assange: Loathed, admired, here to stay
February 1, 2012The secret life of Julian Assange
December 1 2010Court won't reopen Julian Assange's extradition
appeal
June 14 2012**Find More Stories About »**WikiLeaks
Julian Assange

Advertisement

WKILEAKS

Gates: WikiLeaks don't reveal key intel, but risks remain

October 16, 2010 | By Adam Levine CNN

The online leak of thousands of secret military documents from the war in Afghanistan by the website WikiLeaks did not disclose any sensitive intelligence sources or methods, the Department of Defense concluded. However, there is still concern Afghans named in the published documents could be retaliated against by the Taliban.

The assessment, revealed in a letter from Secretary of Defense Robert Gates to the Chairman of the Senate Armed Services Committee, Sen. Carl Levin (D-Michigan), comes after a thorough Pentagon review of the more than 70,000 documents posted to the controversial whistle-blower site in July.

Ads by Google

CIA - Intelligence DegreeEarn an intelligence degree online at American Military University.
www.AMU.APU.S.edu/Intelligence**IT Risk Assessment**Reduce IT Risk and Align Security.
Download Free IT Risk White Paper!
www.Lumension.com/IT-GRC/

Recommend 379 recommendations.



Wikileaks founder Julian Assange, will release more documents.

Advertisement



The letter, provided to CNN, was written August 16 by Gates in response to a query by the senator regarding the leak of classified information.

Gates said the review found most of the information relates to "tactical military operations."

"The initial assessment in no way discounts the risk to national security," Gates wrote. "However, the review to date has not revealed any sensitive intelligence sources and methods compromised by the disclosure."

The defense secretary said that the published documents do contain names of some cooperating Afghans, who could face reprisal by Taliban.

"We assess this risk as likely to cause significant harm or damage to national security interests of the United States and are examining mitigation options," Gates wrote in the letter. "We are working closely with our allies to determine what risks our mission partners may face as a result of the disclosure."

Gates also said there is still the possibility of more documents being published, for which the Pentagon is preparing.

Over the summer, the Pentagon created a team of more than 100 personnel made up of mostly intelligence analysts from various branches of the Defense Department as well as the FBI, who were involved in the round-the-clock review.

WikiLeaks has approximately 15,000 more Afghanistan documents that the site is reviewing because they contain names or other sensitive information. While initially the site founder, Julian Assange, had vowed to publish the additional documents after redaction, there is now some question whether that will happen given the intense criticism WikiLeaks came under after Afghan names were found in the already published files.



Gate... Leaks don't reveal key intel, but risks remain - CNN

Additionally, WikiLeaks is expected to publish as early as next week about 400,000 military documents from the Iraq war that were leaked to the site.

The leaking of the documents raised the immediate ire of military officials, although soon after the posting they questioned the documents' significance. Back in July, Chairman of the Joint Chiefs of Staff Adm. Mike Mullen said he was "appalled" by the leak but said the documents were from previous years up to 2009 and "much has changed since then."

Despite this, the military warned that the naming of Afghans was a huge concern. WikiLeaks has "the blood of some young soldier or that of an Afghan family" on their hands, Mullen said.

In addition to the document review, the military has launched a criminal investigation into the leak. Since the initial publication of the documents, military officials consider Army Pfc. Bradley Manning a prime suspect in the leak. Manning is already being held in Quantico, Virginia, charged with leaking video of an Iraq airstrike to WikiLeaks and removing classified information from military computers.

Act by Google

Manage Operational Risk

Read the Principles for Effective Operational Risk Management Today!
www.IBM.com/OpenPages

Dinner With Barack Obama

Learn how you can have dinner with President Obama.
barackobama.com/dinner-with-barack

Buca di Beppo Specials

Try our Limited Time Specials for Summer. Make a Reservation Online!
www.BucaDiBeppo.com

We recommend

Small Texas community stands by men who killed daughter's alleged abuser CNN.com

Official: Drone strike kills four in Pakistan CNN.com

Computer model shows perfect storm for Obama CNN Politics

Obama asserts executive privilege on some Fast and Furious documents CNN Politics

What Sandusky has said about child rape allegations This Just In

Hebrew National sued over non-kosher allegations CNN US

From around the web

Father Not Charged in Killing of Man Molesting His Daughter, 5 The New York Times

The Death of Marie-Joseph Angélique The Hearin

Nikon announces latest entry-level DSLR, the 24.2-megapixel Nikon D3200 Digital Camera Info

The 5 Most Dangerous Cities in the U.S. AARP.org

10 Signs You May Be in an Emotionally Abusive Relationship HealthCentral.com

State Police Report Arrests in Johnston Providence-New Bedford

[what's hot]

CNN

©2012 Cable News Network, Turner Broadcasting System, Inc. All Rights Reserved

Advertising Practices | Articles CNN.com | Index by Keyword | Index by Date | Terms of Service | Privacy Guidelines

ATTACHMENT E

BBC NEWS

US & CANADA

25 October 2010 Last updated at 13:28 ET

Wikileaks Iraq war documents: the key issues

The Wikileaks website has released some 400,000 secret US military files documenting the conflict in Iraq. A number of issues have been raised by their publication, for example:

Should the documents have remained confidential?

Wikileaks founder Julian Assange says the mass release of documents reveals the truth about the conflict.

"The attack on the truth by war begins long before war starts, and continues long after a war ends," he said, adding that Wikileaks aims "to correct some of that attack".

Wikileaks says it will not disclose where or how it obtained the documents, and that any information which could have been used to identify individuals or sources has been removed before publication.

The organisation says there is no evidence that anyone came to harm as a result of a similar, albeit much smaller, release of material on the conflict in Afghanistan.

But the Pentagon has nevertheless said the documents will be used by America's enemies and will endanger the lives of US personnel serving in Iraq.

It says the reports are "initial, raw observations by tactical units".

"They are essentially snapshots of events, both tragic and mundane, and do not tell the whole story," press secretary Geoff Morrell said in a statement. Moreover, he said, the release "does not bring new understanding" to the conflict.

The US has demanded that Wikileaks hand over the files and remove them from the internet.

The UK's Ministry of Defence has also criticised the release.

Was the US military keeping a record of civilian deaths?

The US military has in the past denied that it has a record of civilian deaths in Iraq. It says that in the heat of battle, casualty reports given by troops, known as field, are not always reliable.

But the released documents show records were kept. The logs, kept and submitted by US military personnel, identify 109,000 violent deaths between 2004 and the end of 2009.

These break down into 66,081 civilians, 23,984 people classed as "enemy", 15,196 members of the Iraqi security forces and 3,771 coalition troops. Some of the logs also contain the names of those who died.

The Iraq Body Count (IBC) project, which has been monitoring civilian deaths throughout the conflict, still has a higher toll, and says it has documented deaths which do not appear in the field reports or are not identified as being civilians.

The Guardian newspaper cites the case of US attacks against insurgents in the city of Fallujah in 2004 - IBC details between 1,226 and 1,362 such deaths during April and November of that year, while the US field reports do not list any civilian deaths.

IBC believes that after cross-checking the leaked reports with its own documents, it has identified 15,000 new civilian deaths.

Hamit Dardagan and John Sloboda, of IBC, wrote in the Guardian that keeping such reports and then making them available to the public was "the correct thing to do, both from a moral and a pragmatic standpoint".

The BBC's Paul Reynolds says the reports appear to show that, despite official misgivings, military units are quite keen to give numbers and that these could in future be compiled by some central counting system.

Was it right for US to simply pass on reports of torture and executions to the Iraqis, rather than taking action?
Critics say the field reports are proof that US military personnel stood by while Iraqi troops tortured and killed civilians.

The US says its troops always acted in accordance with the UN Convention Against Torture and that any evidence of abuse was passed "at the appropriate level" to the Iraqi authorities, who were then responsible for any discipline or retraining.

The Iraqi government said there had been "violations" of official policy by its troops, but that the perpetrators had been punished appropriately.

Correspondents say Washington is coming under pressure to say what its official policy was.

The UK Ministry of Defence has said there was "no place for mistreatment of detainees" and that it would investigate any allegations made against British troops.

The MoD said it had set up a dedicated team to investigate all alleged cases of abuse by UK service personnel in Iraq.

The impact of the leaks on Iraqi politics

With Iraq in political deadlock since inconclusive elections in March, the BBC's Jim Muir in Baghdad says the Wikileaks affair seems to have further envenomed the political situation, making rapid movement towards the formation of a new government even less likely.

The office of Prime Minister Nouri Maliki - who is backed by the country's main Shia coalition, the National Alliance - suggested the leaks were launched or being exploited to undermine his attempt to form that government.

Many of the alleged abuses occurred during the government of Mr Maliki. Many of his critics accuse him of representing Shia sectarian interests.

The Sunni-backed Iraqiya bloc of the former prime minister, Iyad Allawi, clearly hopes the leaks might strengthen his hand. Iraqiya narrowly won the most seats in the general election and Mr Allawi is demanding a 50-50 division of power as the price for joining a government including Mr Maliki.

It seems unlikely the leaks will produce more pressure from ordinary Iraqis on Mr Maliki to reach a compromise with his political rivals.

As our Baghdad correspondent says, Iraqis do not seem to be unduly impressed by the Wikileaks deluge and the alleged links to deaths squads, which had previously been reported.

The legacy of the overthrow of Saddam

The toppling of Saddam Hussein led to him being tried and hanged for his brutal treatment of some of his own people. It also allowed elections to be held.

That gave the Shia majority, which had been dominated under Saddam by the Sunni minority, access to power.

But it also led to a bloody insurgency involving the Sunnis, which left tens of thousands dead. The conflict descended into near sectarian

warfare when Shia militant groups struck back with a campaign of kidnappings and killings.

And, according to Britain's Guardian newspaper, that has left a legacy of torture, summary executions and war crimes. Iraq is a country where abuses of prisoners and opponents are widely believed by its people to be happening, as they were in Saddam's time.

The BBC's defence and security correspondent, Nick Childs, says the leaks raise new questions about the behaviour of the new Iraqi security forces, and about the US military's approach to them.

More US & Canada stories



US economy growth forecast is cut [/news/business-18527347](#)

The US central bank cuts its forecast for economic growth in 2012 and takes steps to reduce long-term borrowing costs.

Obama withholds Fast and Furious files [/news/world-us-canada-18624414](#)

US to seize film director's skeleton [/news/world-us-canada-18618288](#)



BBC © 2012 The BBC is not responsible for the content of external sites. [Read more.](#)

ATTACHMENT F

TUESDAY, AUG 17, 2010 03:15 PM EDT

Are risks from WikiLeaks overstated by government?

National Security Archive historian: "The Pentagon is hyping"

BY ROBERT BURNS, ASSOCIATED PRESS

Although the Pentagon warns that WikiLeaks could have blood on its hands for publishing classified U.S. war documents that name Afghan sources, history shows that similar disclosures have not always led to violence.

It is difficult to find clear-cut examples of the public exposure of informants leading to their deaths, although there are documented cases of a deadly ending to the secret unmasking of foreign agents. Recall the Aldrich Ames espionage case of the early 1990s: The now-jailed CIA turncoat rattled on Soviet informants and at least nine of them were believed executed by the KGB.

The WikiLeaks leak is unrivaled in its scope, but so far there is no evidence that any Afghans named in the leaked documents as defectors or informants from the Taliban insurgency have been harmed in retaliation.

Some private analysts, in fact, think the danger has been overstated.

"I am underwhelmed by this argument. The Pentagon is hyping," says John Prados, a military and intelligence historian who works for the anti-secrecy National Security Archive. He said in an interview that relatively few names have surfaced and it's not clear whether their present circumstances leave them in jeopardy.

Donald P. Gregg, a retired CIA officer and former U.S. ambassador to South Korea, said in an e-mail exchange that the Pentagon's expressions of concern have merit in this case. But he also said his own experience showed that being unmasked as a spy is not always deadly.

"I was named and publicly denounced as a covert CIA officer by East Germany in 1958, and no one, to my knowledge, ever tried to assassinate me," Gregg said.

The Taliban itself, however, has said it is scouring the tens of thousands of leaked documents — mostly raw military intelligence reports — for names of Afghans who sided with the U.S. and NATO against the insurgency. Rep. Jane Harman, a California Democrat, said the leak amounted to handing the Taliban an "enemies list."

"We know the Taliban are harsh and cruel in their treatment of disfavored persons, so it is extremely serious," said Steven Aftergood, an anti-secrecy advocate who writes the Secrecy News blog. "WikiLeaks is giving 'leaks' a bad name by putting people in jeopardy."

Rep. Rush D. Holt, D-N.J., who opposes the U.S. war strategy in Afghanistan, said last week that some of the leaked documents could result in "real harm to real people" — particularly defectors from the Taliban who were interrogated and then released.

"We may presume that after they are released from custody they and their families could be in danger of assassination by other insurgents," Holt wrote in a statement Aug. 10.

In addition to any immediate security risk to Afghans, administration officials say the leak undermines the credibility of U.S. promises to protect the identity of informants. That in turn could hamper U.S. intelligence efforts in the future.

One of the most spectacular cases of exposing foreign agents was Philip Agee's 1975 book, "Inside the Company: CIA Diary."

As a former CIA officer, Agee identified in his book more than 200 agency officers, front companies and foreign agents working for the U.S. abroad. He wrote that this was "one way to neutralize the CIA's support to repression."

He is sometimes accused of responsibility in the death of Richard Welch, the CIA station chief in Athens who was assassinated in 1975 by a Greek terrorist group. Agee and his friends say the accusation is groundless, noting that Welch was not named in Agee's book and that Welch's agency link was publicly known.

His and subsequent exposure of agents led Congress to pass the Intelligence Identities Protection Act of 1982, making it a crime to intentionally reveal the identity of a covert intelligence officer.

Among the earliest expressions of outrage at the Afghan war leaks was from Adm. Mike Mullen, chairman of the Joint Chiefs of Staff. He said he was appalled at the judgment of WikiLeaks.org website founder Julian Assange and the unidentified provider of the secret documents.

"The truth is they might already have on their hands the blood of some young soldier or that of an Afghan family," Mullen told a Pentagon news conference four days after the leak.

Defense Secretary Robert Gates said the U.S. has a moral responsibility to "those who have worked with and put their trust in us in the past, who now may be targeted for retribution."

Last week during a visit aboard a Navy warship in San Diego, Gates told a sailor who asked about the seriousness of the WikiLeaks case: "We don't have specific information of an Afghan being killed yet because of them. But I put emphasis on the word 'yet.'"

Gates' press secretary, Geoff Morrell, said the Pentagon is relaying names of Afghans exposed in the documents to U.S. military commanders in Afghanistan so they can "safeguard those people." It's not clear what steps the U.S. has taken to accomplish this.

The issue could be magnified by an expected WikiLeaks posting soon of thousands of additional leaked documents. Administration officials have said those could be even more compromising.

The vulnerability of locals who work with U.S. forces — openly or secretly — is not just an issue in Afghanistan. A bipartisan group of congressmen and senators called on the Obama administration last week to urgently expand efforts to resettle Iraqis who have worked for U.S. agencies in Iraq, even saying an airlift should be considered. Many of the Iraqis will be targeted for assassination by al-Qaida in Iraq, they said.

“Providing support for our Iraqi allies will advance U.S. national security interests around the world, particularly in Afghanistan, by sending a message that foreign nationals who support our work abroad can expect some measure of protection,” the lawmakers wrote to Secretary of State Hillary Rodham Clinton.

ATTACHMENT G

McClatchy Washington Bureau

[Print This Article](#)

Posted on Sat, Nov. 27, 2010

U.S. officials: New WikiLeaks release will do most harm yet

Nancy A. Yousef | McClatchy Newspapers

last updated: May 14, 2012 05:17:42 PM

WASHINGTON — U.S. diplomats and officials said they're bracing Sunday for at least three newspapers and WikiLeaks to publish hundreds of thousands classified State Department cables that could drastically alter U.S. relations with top allies and reveal embarrassing secrets about U.S. foreign policy.

U.S. diplomats frantically have been reaching out to their counterparts around the world as intelligence officials pleaded with WikiLeaks and the newspapers, including The New York Times, the Guardian in London and Der Spiegel, a German newsweekly, to not publish information that could endanger lives and U.S. policy. Some of the documents are expected to reveal details about how some U.S. diplomats feel about top foreign leaders.

While this is the third time this year that WikiLeaks has released a large batch of documents related to U.S. foreign policy, officials told McClatchy that Sunday's expected release will be far more damaging than the first two combined.

The first batch dealt with Afghanistan and the second with Iraq. Both releases largely gave details about what many thought the U.S. military was doing in those wars. This batch however, is expected to include never released private cables between diplomats.

Publicly, State Department spokesman P.J. Crowley warned that releasing the documents could put "lives and interests at risk." But privately, administration officials are far more concerned about what they contain and implications of releasing them.

NBC News reported Friday that some of the documents would reveal damaging details about U.S. efforts to renegotiate the START nuclear arms treaty with Russia and U.S. anti-terrorism efforts in Yemen.

Speculation is rampant in Washington about what's in the documents.

Germany's Der Spiegel briefly published a story on its website Saturday saying that the documents include 251,287 cables and 8,000 diplomatic directives, most of which date after 2004. About 9,000 documents are from the first two months of this year, the newspaper said.

About 6 percent of the documents were classified as secret, the newspaper said before taking down its story. The majority was unclassified, the newspaper said, but all were intended to remain confidential.

The newspaper said it would release all the documents at 4:30 p.m. EST. WikiLeaks and the newspapers are expected to release the documents and their findings at the same time. However, the release time has changed several times over the past few days.

Secretary of State Hillary Clinton reached out Friday to leaders in Germany, Saudi Arabia, the United Arab Emirates, Britain, France and Afghanistan, Crowley said via Twitter. Diplomats throughout the State Department have spent days reaching out and warning allies of what's coming.

Newspapers in Canada, the United Kingdom, Italy, India, Pakistan, Israel and Belgium, among others, said they expect the leaked documents to include details about U.S. relations with their countries.

Adm. Mike Mullen, the chairman of the Joint Chiefs of Staff, told CNN in an interview to be broadcast Sunday that: "I would hope that those who are responsible for this would, at some point in time, think about the responsibility that they have for lives that they're exposing."

Although WikiLeaks hasn't said how it obtained the documents, U.S. officials think that Army Pfc. Bradley Manning, while a 22-year-old intelligence officer stationed in Iraq, downloaded thousands of documents, at times pretending he was listening to music by Lady Gaga.

Manning and other soldiers had access to the documents as part of an effort by the military to get as much information as possible to soldiers on the battlefield about their communities so that they had the best intelligence possible.

Manning has been charged with illegally downloading thousands of classified documents and is being held in a military jail.

(Shashank Bengali contributed to this article from Baghdad.)

MORE FROM MCCLATCHY

[Wikileaks revelations come as little surprise to many Iraqis](#)

[Sherrod and WikiLeaks: Journalism confronts media frenzy](#)

[McClatchy's national security blog: Nukes & Spooks](#)

[McClatchy's Middle East Diary](#)

McClatchy Newspapers 2010

ATTACHMENT H

The New Yorker

November 29, 2010

The Right to Secrecy

Posted by *George Packer*

What do we learn from the latest WikiLeaks dump, at least according to the Times's privileged and heavily edited account? That the Gulf Arabs are just as nervous about Iran's nuclear program as Israel is, and they want the U.S. to stop it. That Saudi King Abdullah doesn't think much of Iraqi Prime Minister Maliki. That Yemeni President Saleh is happy to claim American airstrikes against Al Qaeda targets as his country's own, and that he doesn't mind whiskey being smuggled into Yemen as long as it's the good stuff. That the Chinese government probably hacked into Google. That Qaddafi never goes anywhere without his Ukrainian "senior nurse."

On the whole, the trove makes American diplomacy look pretty good. Obama's Iran strategy of engagement-leading-to-isolation is shown to have succeeded. Bush—contrary to the impression left on every page of his new memoir—had enough self-awareness about the disaster in Iraq to put the brakes on military action against Iran. And American diplomats are capable of writing blunt, vivid, even amusing assessments of world leaders. Berlusconi is feckless, Sarkozy thin-skinned, Mugabe a megalomaniac: the accounts seem spot-on. The faceless corps of tight-lipped American embassy officials turn out to be an alert and discerning bunch.

Future diplomatic correspondence is going to be a lot more circumspect. The WikiLeaks dump contains (so far) a number of minor embarrassments, a few surprises, a lot of confirmations of what we already pretty much knew, and no scandals. It will make the work of American diplomacy harder for a long time to come. Classification abuse will increase—more cables will be labelled "Top Secret" that should have been labelled "Secret" or "Confidential." Exchanges between American officials and their foreign counterparts will grow less candid and more opaque. The same with cable traffic between U.S. embassies and Washington. There is an undeniable public interest in knowing, for example, that U.S. intelligence believes the Iranians are buying advanced missiles from North Korea, and that Gulf Arab rulers have been privately urging American military action against Iran. The question is, does that interest outweigh the right of U.S. officials to carry out their work with a degree of confidentiality?

Yes—the right. Lawyers, judges, doctors, shrinks, accountants, investigators, and—not least—journalists could not do the most basic tasks without a veil of secrecy. Why shouldn't the same be true of those professionals who happen to be government officials? If WikiLeaks and its super-secretive, thin-skinned, megalomaniacal leader, Julian Assange (is he also accompanied everywhere by a Ukrainian senior nurse?), were uncovering crimes, or scandals, or systemic abuses, there would be no question about the overwhelming public interest in these latest revelations. But the WikiLeaks dump contains no My Lais, no black sites, no Abu Ghraib. The documents simply show State Department officials going about their work over a period of several years. Will we get another update in six months? Will it be worth the damage? Should no government

secret remain secret? Is diplomacy possible when official views have all the privacy of social networking? Assange's stated ambition is to embarrass the U.S. This means that his goals and those of most journalists are not the same. WikiLeaks doesn't trouble itself with these questions. The rest of us, journalists included, should.

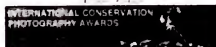
ATTACHMENT I

The Seattle Times Company

The Seattle Times
 Winner of Eight Pulitzer Prizes

Nation & World
[MyJobs](#) | [MyNews](#) | [MyHome](#) | [MySource](#) | [Free Classifieds](#) | [SeattleTimes.com](#)


Search

[Our network sites](#) | [seattletimes.com](#) | [Advanced](#)
[Quick links: Traffic](#) | [Movies](#) | [Restaurants](#) | [Today's events](#) | [Video](#) | [Photos](#) | [Interactives](#) | [Blogs](#) | [Forums](#) | [Subscriber Services](#)
[Contact Us](#)

Originally published Saturday, November 27, 2010 at 4:29 PM

[Comments \(0\)](#) | [E-mail article](#) | [Print](#) | [Share](#)

Secretary of State Clinton contacts countries ahead of WikiLeaks release

Secretary of State Hillary Rodham Clinton has reached out to Germany and a handful of other countries to warn them of the diplomatic fallout ahead of the publication of classified cables and documents, the State Department said Saturday.

By McClatchy Tribune News Service

WASHINGTON — Secretary of State Hillary Rodham Clinton has reached out to Germany and a handful of other countries to contain the diplomatic fallout ahead of the publication of classified cables and documents, the State Department said Saturday.

Clinton contacted leaders in Germany, Saudi Arabia, the United Arab Emirates, France and Afghanistan, spokesman P.J. Crowley posted on his Twitter account. According to earlier media reports, U.S. officials have also contacted officials in Australia, Britain, Canada, Denmark, Israel, Norway and others to discuss the potential impact of the unauthorized leak.

WikiLeaks, the self-proclaimed whistle-blower website, has indicated it will publish nearly 3 million documents. In the past, it has released secret papers through The New York Times, the Guardian and the German magazine Der Spiegel. The release is expected to take place within days but WikiLeaks has not specified the timing.

The State Department is worried the information could include embarrassing details or communications about other countries.

The revelations could be "harmful to the United States and our interests" and "are going to create tension in relationships between our diplomats and our friends around the world," Crowley said earlier this week.

The WikiLeaks release is expected to be the largest leak ever of classified documents. In October, WikiLeaks published nearly 400,000 classified U.S. military documents related to the war in Iraq. It had previously published tens of thousands of military papers about Afghanistan.

The U.S. military arrested Pfc. Bradley Manning and transferred him to the United States in July in connection with leaking classified material to WikiLeaks. U.S. authorities have not said whether Bradley was behind the leaking of the Iraq war logs or the forthcoming State Department documents.

Manning was working as an intelligence analyst in Iraq at the time of his arrest and reportedly had access to classified material.

In hinting that a new release was imminent, WikiLeaks said on Twitter a week ago that it will be "7x the size of the Iraq War Logs." It has documented on its Twitter account press reports about the release and the ongoing discussions between U.S. embassies and their host governments.

The State Department has also informed Congress of the latest pending release, Crowley said. He acknowledged that the State Department "has known all along" that WikiLeaks obtained the diplomatic cables and was bracing for the publication.

PNB's Lucien Postlewaite makes his exit Pacific Northwest Ballet principal dancer Lucien Postlewaite will dance his last performance with the company on June 10 before joining Les Ballets de Monte Carlo in Monaco.

- Seattle hip-hop artist rhymes about recent gun violence
- SPD audio: 911 call from Cafe Racer after shooting
- SPD audio: 911 call from witness at 8th & Seneca shooting
- SPD radio audio: Cafe Racer suspect located
- Crime scenes from Seattle shootings

More videos >

ADVERTISEMENT

ATTACHMENT J

December 2, 2010 1:46 AM

Clinton: WikiLeaks Won't Hurt U.S. Diplomacy

The recent leak of thousands of sensitive U.S. diplomatic cables will have no adverse effect on America's international relations, U.S. Secretary of State Hillary Rodham Clinton declared Wednesday at a security summit.

Clinton said she has discussed the revelations published on the WikiLeaks website with her colleagues at a security summit in Astana, the capital of Kazakhstan. The event is the first major international meeting of leaders and top diplomats since the memos began appearing on the website and in numerous international publications earlier this week.

CBSNews.com Special Report: WikiLeaks

The secret U.S. Embassy memos published by WikiLeaks contain frank details on several leaders attending the Organization for Security and Cooperation in Europe meeting in Astana.

"I have certainly raised the issue of the leaks in order to assure our colleagues that it will not in any way interfere with American diplomacy or our commitment to continuing important work that is ongoing," Clinton said.

"I have not any had any concerns expressed about whether any nation will not continue to work with and discuss matters of importance to us both going forward," she added.

The Obama administration has harshly criticized the leaking of the cables, saying the details in them could put lives at risk.

"I anticipate that there will be a lot of questions that people have every right and reason to ask, and we stand ready to discuss them at any time with our counterparts around the world," Clinton added.

Several officials at the summit echoed her comments.

British Deputy Prime Minister Nick Clegg, who met Wednesday with Clinton, released a statement saying the "recent Wikileaks disclosures would not affect our uniquely strong relationship."

Kazakh Foreign Minister Kanat Saudabayev, commenting on leaked U.S. cables about top officials in his own government, also said "this will have no bearing on our strategic relationship."

In an interview with Time magazine, WikiLeaks founder Julian Assange said Clinton "should resign" if it's shown she ordered U.S. diplomats to gather information on other foreign officials, including those from the United Nations.

More on WikiLeaks

ATTACHMENT K



U.S. Department of Defense
Office of the Assistant Secretary of Defense (Public Affairs)

News Transcript

On the Web:

<http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=4726>

Media contact: +1 (703) 697-5131/697-5132

Public contact:

<http://www.defense.gov/landing/comment.aspx>

or +1 (703) 571-3343

Presenter: Secretary of Defense Robert M. Gates and Chairman, Joint Chiefs of Staff Adm. Mullen

November 30,
2010

DOD News Briefing with Secretary Gates and Adm. Mullen from the Pentagon

SEC. GATES: Good afternoon.

This past February, I established a high-level working group to review the issues associated with implementing a repeal of the "don't ask, don't tell" law regarding homosexual men and women serving in the military, and based on those findings to develop recommendations for implementation should the law change. The working group has completed their work, and today the department is releasing their report to the Congress and to the American public.

Admiral Mullen and I will briefly comment on the review's findings and our recommendations for the way ahead.

We will take some questions. And then the working group's co-chairs, General Counsel Jeh Johnson and Army General Carter Ham, will provide more detail on the report, and answer any questions you might have on methodology, data and recommendations.

When I first appointed Mr. Johnson and General Ham to assume this duty, I did so with the confidence that they would undertake this task with the thoroughness, the seriousness, professionalism and objectivity befitting a task of this magnitude and consequence. I believe that a close and serious reading of this report will demonstrate they've done just that. We are grateful for the service they have rendered in taking on such a complex and controversial subject.

The findings of their report reflect nearly 10 months of research and analysis along several lines of study, and represent the most thorough and objective review ever of this difficult policy issue and its impact on the American military.

First, the group reached out to the force to better understand their views and attitudes about a potential repeal of the "don't ask, don't tell" law. As was made clear at the time and is worth repeating today, this outreach was not a matter of taking a poll of the military to determine whether the law should be changed. The very idea of asking the force to in effect vote on such a matter is antithetical to our system of government, and would have been without precedent in the long history of our civilian-led military.

The president of the United States, the commander in chief of the armed forces, made his position on this matter clear, a position I support. Our job as the civilian and military leadership of the Department of Defense was to determine how best to prepare for such a change should the Congress change the law.

Nonetheless, I thought it critically important to engage our troops and their families on this issue, as ultimately it will be they who will determine whether or not such a transition is successful. I believe that we had to learn the attitudes, obstacles and concerns that would need to be addressed should the law be changed. We could do this only by reaching out and listening to our men and women in uniform and their families.

The working group undertook this through a variety of means, from a mass survey answered by tens of thousands of troops and their spouses to meetings with small groups and individuals, including hearing from those discharged under the current law.

Mr. Johnson and General Ham will provide more detail on the results of the survey of troops and their families.

But in summary, a strong majority of those who answered the survey — more than two-thirds — do not object to gays and lesbians serving openly in uniform. The findings suggest that for large segments of the military, repeal of "don't ask, don't tell," though potentially disruptive in the short term, would not be the wrenching, traumatic change that many have feared and predicted.

The data also shows that within the combat arms specialties and units, there is a higher level of discontent, of discomfort and resistance to changing the current policy. Those findings and the potential implications for America's fighting forces remain a source of concern to the service chiefs and to me. I'll discuss this later.

Second, the working group also examined thoroughly all the potential changes to the department's regulations and policies dealing with matters such as benefits, housing, relationships within the ranks, separations and discharges. As the co-chairs will explain in a few minutes, the majority of concerns often raised in association with the repeal — dealing with sexual conduct, fraternization, billeting arrangements, marital or survivor benefits — could be governed by existing laws and regulations.

Existing policies can and should be applied equally to homosexuals as well as heterosexuals. While a repeal would require some changes to regulations, the key to success, as with most things military, is training, education, and, above all, strong and principled leadership up and down the chain of command.

Third, the working group examined the potential impact of a change in the law on military readiness, including the impact on unit cohesion, recruiting and retention, and other issues critical to the performance of the force. In my view, getting this category right is the most important thing we must do.

The U.S. armed forces are in the middle of two major military overseas campaigns — a complex and difficult drawdown in Iraq, a war in Afghanistan — both of which are putting extraordinary stress on those serving on the ground and their families. It is the well-being of these brave young Americans, those doing the fighting and the dying since 9/11, that has guided every decision I have made in the Pentagon since taking this post nearly four years ago. It will be no different on this issue. I am determined to see that if the law is repealed, the changes are implemented in such a way as to minimize any negative impact on the morale, cohesion and effectiveness of combat units that are deployed, about to deploy to the front lines.

With regards to readiness, the working group report concluded that overall and with thorough preparation — and I emphasize thorough preparation — there is a low risk from repealing "don't ask, don't tell." However, as I mentioned earlier, the survey data showed that a higher proportion — between 40 (percent) and 60 percent — of those troops serving in predominately all-male combat specialties — mostly Army and Marines, but including the Special Operations formations of the Navy and the Air Force — predicted a negative effect on unit cohesion from repealing the current law.

For this reason, the uniform service chiefs are less sanguine about the working — than the working group about the level of risk of repeal with regard to combat readiness.

The views of the chiefs were sought out and taken seriously by me and by the authors of this report. The chiefs will also have the opportunity to explain their — to provide their expert military advice to the Congress, as they have to me and to the president. Their perspective deserves serious attention and consideration, as it reflects the judgment of decades of experience and the sentiment of many senior officers.

In my view, the concerns of combat troops as expressed in the survey do not present an insurmountable barrier to successful repeal of "don't ask, don't tell." This can be done and should be done without posing a serious risk to military readiness. However, these findings do lead me to conclude that an abundance of care and preparation is required if we are to avoid a disruptive and potentially dangerous impact on the performance of those serving at the tip of the spear in America's wars.

This brings me to my recommendations on the way ahead. Earlier this year, the House of Representatives passed legislation that would repeal "don't ask, don't tell" after a number of steps take place, the last being certification by the president, the secretary of Defense and the chairman that the new policies and regulations were consistent with the U.S. military's standards of readiness, effectiveness, unit cohesion, and recruiting and retention.

Now that we have completed this review, I strongly urge the Senate to pass this legislation and send it to the president for signature before the end of this year.

I believe this is a matter of some urgency because, as we have seen in the past year, the federal courts are increasingly becoming involved in this issue. Just a few weeks ago, one lower court ruling forced the department into an abrupt series of changes that were no doubt confusing and distracting to men and women in the ranks. It is only a matter of time before the federal courts are drawn once more into the fray, with the very real possibility that this change would be

imposed immediately by judicial fiat -- by far the most disruptive and damaging scenario I can imagine, and one of the most hazardous to military morale, readiness and battlefield performance.

Therefore, it is important that this change come via legislative means; that is, legislation informed by the review just completed. What is needed is a process that allows for a well-prepared and well-considered implementation -- above all, a process that carries the imprimatur of the elected representatives of the people of the United States.

Given the present circumstances, those that choose not to act legislatively are rolling the dice that this policy will not be abruptly overturned by the courts. The legislation presently before the Congress would authorize a repeal of the "don't ask, don't tell" pending a certification by the president, secretary of Defense and the chairman. It would not harm military readiness.

Nonetheless, I believe that it would be unwise to push ahead with full implementation of repeal before more can be done to prepare the force -- in particular, those ground combat specialties and units -- for what could be a disruptive and disorienting change.

The working group's plan, with a strong emphasis on education, training and leader development, provides a solid road map for a successful full implementation of repeal, assuming that the military is given sufficient time and preparation to get the job done right.

The department has already made a number of changes to regulations that within existing law applied more exacting standards to procedures, investigating or separating troops for suspected homosexual conduct -- changes that have added a measure of common sense and decency to a legally and morally fraught process.

I would close on a personal note and a personal appeal. This is the second time that I have dealt with this issue as a leader in public life, the prior case being in CIA in 1992 when I directed that openly gay applicants be treated like all other applicants; that is, whether as individuals they met our competitive standards. That was and is a situation significantly different in circumstance and consequence than confronting -- than that confronting the United States armed forces today.

Views toward gay and lesbian Americans have changed considerably during this period, and have grown more accepting since "don't ask, don't tell" was first enacted. But feelings on this matter can still run deep and divide often starkly along demographic, cultural and generational lines, not only in society as a whole but in the uniformed ranks as well.

For this reason, I would ask, as Congress takes on this debate, for all involved to resist the urge to lure our troops and their families into the politics of this issue. What is called for is a careful and considered approach, an approach that to the extent possible welcomes all who are qualified and capable of serving their country in uniform, but one that does not undermine out of haste or dogmatism those attributes that make the U.S. military the finest fighting force in the world.

The stakes are too high for a nation under threat, for a military at war, to do any less.

Admiral?

ADM. MULLEN: Thank you, Mr. Secretary.

I, too, wish to thank Jeh Johnson and Carter Ham, as well as everyone involved in the working group, for their extraordinary efforts over much of the past year. I fully endorse their report, its findings and the implementation plan recommended by the working group.

The working group was given a tall order -- indeed, nothing less than producing the first truly comprehensive assessment of not only the impact of repeal of the law governing "don't ask, don't tell," but also about how best to implement a new policy across the joint force. As the secretary indicated, the working group surveyed our troops and their spouses, consulted proponents and opponents of repeal, and examined military experience around the world. They also spoke with serving gays and lesbians, as well as former members of the military who are gay and lesbian. The result is one of the most expansive studies ever done on military personnel issues, and I applaud the time that was taken to arrive at solid, defensible conclusions.

More critically, I was gratified to see that the working group focused their findings and recommendations, rightly, on those who would be most affected by a change in the law: our people, all of our people. And so for the first time, the chiefs and I have more than just anecdotal evidence and hearsay to inform the advice we give our civilian leaders. We've discussed this issue extensively amongst ourselves and with the secretary, and the chiefs and I met with the president as recently as yesterday.

I only want to add three points to what the secretary's already laid out.

First, I think it's noteworthy that the working group found strong leadership to be the single most important factor in implementing any repeal. That may sound fairly obvious, but it is a key, critical point.

We all have our opinions, and those opinions matter. This is without question a complex social and cultural issue. But at the end of the day, whatever the decision of our elected leaders may be, we in uniform have an obligation to follow orders. When those orders involve significant change such as this would, we need to find ways to lead the way forward. Our troops and their families expect that from us, and I think the American people do as well.

Second, we've heard loud and clear that our troops also expect us to maintain high standards of conduct and professionalism, both as we move forward in this debate and should repeal occur. We treat people with dignity and respect in the armed forces, or we don't last long. No special cases, no special treatment, if we're going to continue to comport ourselves with honor and hold ourselves accountable across the board to impeccably high standards, repeal or no repeal.

Finally, the report shows that however low the overall risk of repeal may be with respect to readiness, cohesion and retention, it is not without its challenges. We can best address those challenges by having it within our power and our prerogative to manage the implementation process ourselves.

Should repeal occur, I share the secretary's desire that it come about through legislation — through the same process with which the law was enacted, rather than precipitously through the courts. I further hope that such debate in the Congress will be as fully informed by the good work done in this report as my advice to the secretary and to the president is.

Thank you.

Q: Secretary Gates, you said it would be unwise to proceed with repeal until there is more groundwork. How long do you envision that process lasting? And is this a concern and a recommendation that is shared by the White House in — as far as once Congress acts there still being a period in which the policy is in place?

Admiral Mullen, do you also share that recommendation?

SEC. GATES: Well, first of all, just to be clear, what we're talking about is that, should the Congress vote to repeal the law, what we are asking for is the time subsequent to that to prepare adequately before the change is implemented in the force. How long that would take, frankly, I don't know. There is the — the report, as you will see in the implementation plan, lays out an ambitious agenda of things that need to be done, including not only leadership training but training of a military force of over 2 million people.

I would say this. I think we all would expect that if this law is implemented, the president would be — is — if repeal is passed, the president would be watching very closely to ensure that we don't dawdle or try to slow-roll this. So I think his expectation would be that we would prepare as quickly as we properly and comprehensively could, and then we would be in a position to move toward the certification. But how long that would take I think — I don't know.

ADM. MULLEN: There will — there will be level — there is a level of risk here, as is laid out in the report. And I would hope you spend as much time on the implementation plan as the report, because the implementation plan certainly from all the military leadership is strongly endorsed should this law change.

And it is in that implementation plan that the risk levels are mitigated, and principally mitigated through leadership — certainly the training, the guidance, but the engagement of the leadership. And having enough time to do that is critically important as we would look at implementation. That's what really mitigates any risk that's out there.

Q: Mr. Secretary, you said the chiefs are less sanguine than the working group. What specifically have they told you about their concerns? And why in a time of war accept any increase in the level of risk?

SEC. GATES: Well, the chiefs will speak for themselves on Friday. And the chairman has spent much more time with them than I have on this. I think — I think it's fair to say that their concerns revolve around stress on a force after nearly 10 years of war. And I think they are concerned about the higher levels of negative response from the ground combat units and the Special Operations units that I have talked about in my — in my remarks.

I think that — I would just like to go back and underscore the chairman's point, and that is the level of risk is tied intimately to the quality of preparation. And to do this — so I guess I would put it this way: If a court ordered us to do this tomorrow, I believe the force — the risk to the force would be high, if we had no time to prepare.

If we have plenty of time to prepare the force, to prepare the leadership, I think the more effectively we do that preparation the lower the risk.

Chairman?

ADM. MULLEN: I've engaged, actually, many, many times with the chiefs over the last — over the last many months, and so we've had very, very extensive discussions about this. And from the standpoint of a change in the law — I mean, my perspective is, as what I would call my — certainly was my personal opinion, is now my professional view, that this is a policy change that we can make. And we can do it in a relatively low-risk fashion, given the time and given the ability to mitigate whatever risk is out there through strong leadership.

In fact, part of this is the fact that we have been at war for so long. We have — one of the discussions about this is affecting combat effectiveness or combat readiness. I've never been associated with a better military than we are right now and better military leaders. And I have tremendous confidence that should this change, that they'll be able to implement it, very specifically.

Q: That's true, but what about the other chiefs?

ADM. MULLEN: Well, again, the chiefs will speak for themselves on Friday.

Q: Mr. Secretary, you raised the issue of combat arms, and the report shows that of those polled, 50 percent in Army combat arms are opposed, 60 percent in Marine combat arms. And there's also the issue of chaplains. The report says that there's very strong opposition among the chaplains there as well.

What would you say to both groups? How would you deal with this with both groups?

SEC. GATES: Well, the interesting — one of the other considerations in this that the — that the report revealed is even in combat arms units, those who — among those who believed they had served with a gay person before, the level of comfort with going forward was something like 90 percent.

So part of this is a question of unfamiliarity. Part of it is stereotypes. And part of it is just sort of inherent resistance to change when you don't know what's on the other side.

And so I think — I think that the contrast between the significant levels of concern for those who had — who said they had never served with someone who is gay as opposed to those who had is an important consideration. But what I would say to them is, you know, frankly, if the Congress of the United States repeals this law, this is the will of the American people, and you are the American military, and we will do this, and we will do it right, and we will do everything in our power to mitigate the concerns that you have.

Q: And on the chaplains?

SEC. GATES: Saying —

Q: The report — (inaudible) — a very large number view homosexuality as a sin or an abomination.

SEC. GATES: And the report — the report identifies that the chaplains already serve in a force many of whose members do not share their values, who do not share their beliefs. And there is an obligation to care for all. But it also is clear that the chaplains are not going to be asked to teach something they don't believe in. And so I think that the — I think the report is pretty clear on that.

Q: Thank you. Non-"don't ask, don't tell" question quick?

SEC. GATES: Sure.

Q: WikiLeaks. Post-WikiLeaks reaction. What's your sense on whether the information-sharing climate and environment created after 9/11 to encourage greater cooperation and transparency among the intelligence communities and the military led to these three massive data dumps?

And how concerned are you now there may be an overreaction to clamp down on information dispersal because of the disclosures?

SEC. GATES: One of the common themes that I heard from the time I was a senior agency official in the early 1980s in every military engagement we were in was the complaint of the lack of adequate intelligence support. That began to change with the Gulf War in 1991, but it really has changed dramatically after 9/11.

And clearly the finding that the lack of sharing of information had prevented people from, quote/unquote, "connecting the dots" led to much wider sharing of information, and I would say especially wider sharing of information at the front, so that no one at the front was denied — in one of the theaters, Afghanistan or Iraq — was denied any information that might possibly be helpful to them. Now, obviously, that aperture went too wide. There's no reason for a young officer at a forward operating post in Afghanistan to get cables having to do with the START negotiations. And so we've taken a number of mitigating steps in the department. I directed a number of these things to be undertaken in August.

First, the — an automated capability to monitor workstations for security purposes. We've got about 60 percent of this done, mostly in — mostly stateside. And I've directed that we accelerate the completion of it.

Second, as I think you know, we've taken steps in CENTCOM in September and now everywhere to direct that all CD and DVD write capability off the network be disabled. We have — we have done some other things in terms of two-man policies — wherever you can move information from a classified system to an unclassified system, to have a two-person policy there.

And then we have some longer-term efforts under way in which we can — and, first of all, in which we can identify anomalies, sort of like credit card companies do in the use of computer; and then finally, efforts to actually tailor access depending on roles.

But let me say — let me address the latter part of your question. This is obviously a massive dump of information. First of all, I would say unlike the Pentagon Papers, one of the things that is important, I think, in all of these releases, whether it's Afghanistan, Iraq or the releases this week, is the lack of any significant difference between what the U.S. government says publicly and what these things show privately, whereas the Pentagon Papers showed that many in the government were not only lying to the American people, they were lying to themselves.

But let me — let me just offer some perspective as somebody who's been at this a long time. Every other government in the world knows the United States government leaks like a sieve, and it has for a long time. And I dragged this up the other day when I was looking at some of these prospective releases. And this is a quote from John Adams: "How can a government go on, publishing all of their negotiations with foreign nations, I know not."

To me, it appears as dangerous and pernicious as it is novel."

When we went to real congressional oversight of intelligence in the mid-'70s, there was a broad view that no other foreign intelligence service would ever share information with us again if we were going to share it all with the Congress. Those fears all proved unfounded.

Now, I've heard the impact of these releases on our foreign policy described as a meltdown, as a game-changer, and so on. I think — I think those descriptions are fairly significantly overwrought. The fact is, governments deal with the United States because it's in their interest, not because they like us, not because they trust us, and not because they believe we can keep secrets. Many governments — some governments deal with us because they fear us, some because they respect us, most because they need us. We are still essentially, as has been said before, the indispensable nation.

So other nations will continue to deal with us. They will continue to work with us. We will continue to share sensitive information with one another.

Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest.

Q: And on that same subject. On that same subject. Did either of you reach out to any of your counterparts in advance of this leak and warn them, or even apologize in advance for what might come out?

SEC. GATES: I didn't.

ADM. MULLEN: I did.

Q: Who was it?

ADM. MULLEN: To General Kayani in Pakistan.

SEC. GATES: Yeah?

Q: Sir, you've said that — you know, on "don't ask, don't tell" — you've said that now is the time to do this, largely because of the threat of legal action. I'm just wondering, if that legal action wasn't looming, how much do you think that this would — this is the right thing to do now?

And I'm wondering just how hard you intend to lobby those on the Hill to get them to sway to the other side.

SEC. GATES: Well, you know, I don't spend much time thinking about the world as I wish it were. The reality is the court issue is out there, and, in my view, does lend urgency to this.

You know, the question was — has been raised, well, maybe the courts would give us time, to which my answer is, maybe, maybe not. We just don't know. But the one path we know gives us the time and the flexibility to do this is the legislative path. And I don't know how fast the courts are going to move on this, but what we've seen seems to be more and more action in the courts in the last year or two. And that's what gives me a sense of urgency about. My greatest fear is what almost happened to us in October, and that is being told to implement a change of policy overnight.

Q: Yeah. Mr. Secretary, Senator McCain is now arguing that this report is the wrong report, and that it won't get to the bottom of how this could — the repeal could affect unit cohesion or morale. I'm wondering if you or Admiral Mullen have any reaction to that response to the report.

SEC. GATES: Well, I think — I think that, in this respect — and I obviously have a lot of admiration and respect for Senator McCain — but in this respect, I think that he's mistaken. I think this report does provide a sound basis for making decisions on this law.

Now, people can draw different conclusions out of this report; the comments, for example, in the — in the evaluation in the report of the higher levels of concern for — among the combat arms units and in the Marine Corps and so on.

So people can read this and potentially come to different conclusions, but in terms of the data and in terms of the views of the force, it's hard for me to imagine that you could come up with a more comprehensive approach.

We had — we had something on the order of 145,000 people in uniform answer the questionnaire, the survey. We had something on the order of 40,000 to 45,000 spouses respond to the — to that survey. Tens of thousands of people reached in other ways. So I think there is no comparable source of information or data on attitudes in the force than this report, and it's hard for me to imagine another effort taking a much different approach than this report did.

ADM. MULLEN: And its main thrust was on combat effectiveness, mission effectiveness, readiness, unit cohesion, et cetera. And that data — again, I agree with the Secretary, you can certainly pick parts of it that read — you might want to read differently. But the data's very compelling, in particular with respect to those issues. I mean, that was the main reason for the report.

Q: I wonder if you could talk a little bit more about how you would see this implemented and what you mean by giving time. For example, would you, say, not have openly gay — if the law is changed, would you not put openly gay servicemembers into units that units that are about to deploy to Afghanistan in 2011 or so? Would you — would you take — would you integrate the non-combat arms units first? I mean, what — could you describe a little bit more of what your implementation plan would be?

SEC. GATES: Well, first of all, the repeal of the law would not, as I understand it — now I'm not a lawyer — but as I understand it — and maybe Jeh Johnson can address this question for you more authoritatively when he comes up here.

But as I understand it, until we certify, until the president, the secretary of Defense and the chairman of the Joint Chiefs certify that we — that the U.S. military is ready to implement the law, the repeal, the existing — the currently existing rules would continue to apply. And so you would have a period of preparation, if you will, that, as I indicated earlier, I don't know necessarily how long that would take.

ADM. MULLEN: And, Julian — and from my perspective, we are one military. We are one military.

SEC. GATES: Two more questions. Yeah.

Q: Mr. Secretary, you have spoken quite clearly about how you support the president's position on this, and how you're urging the Senate to act, and how this needs to be done in an orderly and measured way.

But you haven't said so much over time about your personal beliefs on "don't ask, don't tell." Do you feel personally that it's been unjust or wrong for gays and lesbians not to be able to serve their country openly? Or are you comfortable with the idea of openly integrating the military?

SEC. GATES: I think that — in my view — one of the things that is most important to me is personal integrity. And a policy or a law that in effect requires people to lie gives me — gives me a problem. And so I think it's — I mean, we spend a lot of time in the military talking about integrity and honor and values.

Telling the truth is a pretty important value in that scale. It's a very important value. And so for me, and I thought the admiral was — that Admiral Mullen was eloquent on this last February — a policy that requires people to lie about themselves somehow seems to me fundamentally flawed.

Last question.

Q: Earlier in the process, General Conway, when raising concerns about this, floated the idea of separate barracks and said that, you know, Marines might not be comfortable sharing barracks with openly gay troops. Is that even on the table, or is that — would the idea of separate barracks, separate housing, separate showers just be off the table?

SEC. GATES: We can get into the details of that — or you can with Jeh and General Ham. But the bottom line of the report is no separate facilities.

Thank you.

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC
U.S. Army, [REDACTED]
Headquarters and Headquarters Company, U.S.
Army Garrison, Joint Base Myer-Henderson Hall,
Fort Myer, VA 22211

**DEFENSE REQUESTED
INSTRUCTION:
SPECIFICATIONS 13 AND 14 OF
CHARGE II**

DATED: 22 June 2012

1. The defense requests the following instructions to be given to the panel regarding Specifications 13 and 14 of Charge II:¹

Court Instructions

In Specification 13 and Specification 14 of Charge II, the accused is charged with the offense of Exceeding Authorized Access to a Computer, a violation of 18 U.S.C. Section 1030(a)(1). To find the accused guilty of this offense with regards to Specification 13, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

(1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, accessed a computer with authorization, but exceeded his authority in accessing the information in question on a Secret Internet Protocol Router network computer;

(2) That the accused knowingly exceeded his authorized access;

(3) That the accused, by means of such conduct, obtained information protected against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data to wit: more than 75 classified United States Department of State cables, with the intent to use such information against the interests of the United States;

(4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the information obtained to a person not entitled to receive it (or willfully retained that information and failed to deliver it to the officer or employee of the United States entitled to receive it); and

¹ This motion does not propose instructions on any potential lesser-included offense (LIO) for the Section 1030(a)(1) violations alleged in Specifications 13 and 14 of Charge II because the Government has not yet identified the act that would constitute the LIO. However, regardless of the act identified by the Government, the Defense submits that any LIO of these offenses would be akin to a violation of Article 92, UCMJ, and would accordingly carry a maximum penalty of two years imprisonment.

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 1030(a)(1); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc); *United States v. Alyenikov*, 737 F.Supp.2d 173 (S.D.N.Y. 2010); Military Judges Benchbook, DA Pam 27-9; Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.1030A. Ninth Circuit: Ninth Circuit Model Criminal Jury Instructions 8.95. Eleventh Circuit: Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 42.1.

Similarly, to find the accused guilty of this offense with regards to Specification 14, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 18 February 2010, accessed a computer with authorization, but exceeded his authority in accessing the information in question on a Secret Internet Protocol Router network computer;
- (2) That the accused knowingly exceeded his authorized access;
- (3) That the accused, by means of such conduct, obtained information protected against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data to wit: a classified Department of State cable titled "Reykjavik 13," with the intent to use such information against the interests of the United States;
- (4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the information obtained to a person not entitled to receive it (or willfully retained that information and failed to deliver it to the officer or employee of the United States entitled to receive it); and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 1030(a)(1); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc); *United States v. Alyenikov*, 737 F.Supp.2d 173 (S.D.N.Y. 2010); Military Judges Benchbook, DA Pam 27-9; Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.1030A. Ninth Circuit: Ninth Circuit Model Criminal Jury Instructions 8.95. Eleventh Circuit: Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 42.1.

Court Definitions

(1) Exceeding Authorized Access to a Computer

The first element that the government must prove beyond a reasonable doubt is that the accused accessed a computer with authorization, but exceeded his authority in accessing the information in question.

In this case, the government charges that the accused, while authorized to access the computer, exceeded his authority in accessing the information in question. Under the statute, this requires that the government prove beyond a reasonable doubt that the accused had access to the computer, and used that access to obtain or alter information in the computer that the accused was not entitled to obtain or alter. In other words, the term 'exceeds authorized access' applies to 'inside hackers', individuals whose initial access to a computer is authorized but who access unauthorized information or files."

This element is not satisfied by mere misuse or misappropriation of information that the accused was authorized to access. Nor does it apply where the accused accesses information that he was authorized to access, but in an unauthorized manner. Rather, this element is only satisfied where the accused is authorized to access the computer and obtains or alters information on that computer that the accused is not entitled to obtain or alter.

If you find that the accused had authorization to access the computer and to obtain the information, you must find the accused not guilty.

Authority: 18 U.S.C. § 1030(e)(6); H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 22 (1984); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc); *United States v. Alyenikov*, 737 F.Supp.2d 173 (S.D.N.Y. 2010).

(2) Knowing Conduct

The second element that the government must prove beyond a reasonable doubt is that the accused acted knowingly in exceeding his authorized access to the computer.

"Knowingly" means to act voluntarily or deliberately, rather than mistakenly or inadvertently.

The question of whether a person acted knowingly is a question of fact for you to determine. The question involves the accused's state of mind.

As a practical matter, then, in order to sustain the charges against the accused, the government must establish beyond a reasonable doubt that the accused knew that he was exceeding authorized access in accessing the information.

If you find that the accused did not know he was acting without authorization (or exceeding authorization) or that the accused actually believed he was acting with authorization (or within his authorization), then you must find the accused not guilty.

Authority: 18 U.S.C. § 1030(a)(1); H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 20 (1984); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc); *United States v. Alyenikov*, 737 F.Supp.2d 173 (S.D.N.Y. 2010); Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.1030A. Ninth Circuit: Ninth Circuit Model Criminal Jury Instructions 8.95. Eleventh Circuit: Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 42.1.

(3) Obtaining Protected or Restricted Information

The third element that the government must prove beyond a reasonable doubt is that the accused obtained information protected against unauthorized disclosure for reasons of national defense or foreign relations or any restricted data, with the intent to use such information against the interests of the United States.

The United States may determine that information requires protection against unauthorized disclosure for reasons of national defense or foreign relations either by Executive Order or by statute.

The government must also establish beyond a reasonable doubt that, at the time he obtained the protected or restricted information, the accused had reason to believe that the information could be used against the interests of the United States or to the advantage of a foreign nation.

If you find that the information allegedly obtained by the accused was not protected against disclosure for reasons of national defense or foreign relations and was not restricted data, or that the accused did not have a reason to believe that the information could be used against the interests of the United States or to the advantage of a foreign nation, you must find the accused not guilty.

Authority: 18 U.S.C. § 1030(a)(1); H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 21 (1984); Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.1030A. Ninth Circuit: Ninth Circuit Model Criminal Jury Instructions 8.95. Eleventh Circuit: Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 42.1.

(4) Willfully Communicated of Improperly Obtained Information

The fourth element that the government must prove beyond a reasonable doubt is that the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver, transmit) the protected or restricted information obtained to any person [or entity] not entitled to receive it (or willfully retained that information and failed to deliver it to the officer or employee of the United States entitled to receive it).

To act willfully means to act knowingly and purposefully, with an intent to do something that the law forbids, that is to say, with a bad purpose either to disobey or disregard the law. There is no requirement that the accused acted for financial gain.

If you find that the accused did not willfully communicate (or deliver or transmit or cause or attempt to communicate, deliver, or transmit) the protected or restricted information to a person or entity not entitled to receive it, you must find the accused not guilty.

Authority: 18 U.S.C. § 1030(a)(1); Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.1030A. Ninth Circuit: Ninth Circuit Model Criminal Jury Instructions 8.95. Eleventh Circuit: Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 42.1.

(5) Prejudicial to Good Order and Discipline and Service Discrediting Conduct

The final element of the offense that the government must establish beyond a reasonable doubt is that the accused's conduct was prejudicial to good order and discipline and of a nature to bring discredit upon the armed forces.

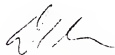
"Conduct prejudicial to good order and discipline" is conduct which causes a reasonable direct and obvious injury to good order and discipline. "Service discrediting conduct" is conduct which tends to harm the reputation of the service or lower it in public esteem.

If you find that the accused's conduct was not prejudicial to good order and discipline and/or was not of a nature to bring discredit upon the armed forces, you must find the accused not guilty.

Authority: Military Judges' Benchbook – notes under Article 134

2. The Defense respectfully requests the above instructions and definitions be given by the Court.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

DEFENSE REQUESTED

INSTRUCTION:

SPECIFICATIONS 2, 3, 5, 7, 9, 10,
11 AND 15 OF CHARGE II

DATED: 22 June 2012

1. The defense requests the following instructions to be given to the panel regarding Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II:

Court Instructions

In Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II, the accused is charged with the offense of Espionage, a violation of 18 U.S.C. Section 793(e). To find the accused guilty of this offense with regards to Specification 2, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 5 April 2010, have unauthorized possession of (or control over or access to) information;
- (2) That the information was relating to the national defense, to wit: a video file named "12 JUL 07 CA ENGAGEMENT ZONE 30 GC Anyone.avi";
- (3) That the accused knew or had a reason to believe that the named video could be used to the injury of the United States or to the advantage of any foreign nation;
- (4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the named video to [a person or entity], who was not entitled to receive it; and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 793(e). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979); Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 3, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 22 March 2010 and on or about 26 March 2010, have unauthorized possession of (or control over or access to) information;
- (2) That the information was relating to the national defense, to wit: more than one classified memorandum produced by a United States government intelligence agency;
- (3) That the accused knew or had a reason to believe that the named memoranda could be used to the injury of the United States or to the advantage of any foreign nation;
- (4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the named memoranda to [a person or entity], who was not entitled to receive it; and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 793(e). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979); Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 5, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 9 February 2010, have unauthorized possession of (or control over or access to) information;
- (2) That the information was relating to the national defense, to wit: more than twenty classified records from the Combined Information Data Network Exchange Iraq database;
- (3) That the accused knew or had a reason to believe that the named information could be used to the injury of the United States or to the advantage of any foreign nation;
- (4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the named information to [a person or entity], who was not entitled to receive it; and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 793(e). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979); Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 7, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 9 February 2010, have unauthorized possession of (or control over or access to) information;
- (2) That the information was relating to the national defense, to wit: more than twenty classified records from the Combined Information Data Network Exchange Afghanistan database;
- (3) That the accused knew or had a reason to believe that the named information could be used to the injury of the United States or to the advantage of any foreign nation;
- (4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the named information to [a person or entity], who was not entitled to receive it; and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 793(e). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979); Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 9, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 8 March 2010 and on or about 27 May 2010, have unauthorized possession of (or control over or access to) information;
- (2) That the information was relating to the national defense, to wit: more than three classified records from a United States Southern Command database;
- (3) That the accused knew or had a reason to believe that the named information could be used to the injury of the United States or to the advantage of any foreign nation;
- (4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the named information to [a person or entity], who was not entitled to receive it; and

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 793(e). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979); Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 10, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

(1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 11 April 2010 and on or about 27 May 2010, have unauthorized possession of (or control over or access to) information;

(2) That the information was relating to the national defense, to wit: more than five classified records relating to a military operation in Farah Province, Afghanistan occurring on or about 4 May 2009;

(3) That the accused knew or had a reason to believe that the named information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the named information to [a person or entity], who was not entitled to receive it; and

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 793(e). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979); Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 11, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

(1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 8 January 2010, have unauthorized possession of (or control over or access to) information;

(2) That the information was relating to the national defense, to wit: a file named "BE22 PAX.zip" containing a video named "BE22 PAX.wmv";

(3) That the accused knew or had a reason to believe that the named information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the named information to [a person or entity], who was not entitled to receive it; and

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 793(e). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979); Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 15, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

(1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 15 March 2010, have unauthorized possession of (or control over or access to) information;

(2) That the information was relating to the national defense, to wit: a classified record produced by a United States Army intelligence organization, dated 18 March 2008;

(3) That the accused knew or had a reason to believe that the named information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered or transmitted or attempted to communicate, deliver or transmit) the named information to [a person or entity], who was not entitled to receive it; and

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 793(e). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979); Military Judges Benchbook, DA Pam 27-9.

Court definitions

(1) Possession

The first element of the offense that the government must prove beyond a reasonable doubt is that the accused had unauthorized possession of (or control over or access to) the charged

information.

The word "possession" is a commonly used and commonly understood word. It means the act of having or holding property or the detention of property in one's power or command. Possession may mean actual physical possession or constructive possession. A person has constructive possession of something if he knows where it is and can get it any time he wants, or otherwise can exercise control over it.

A person has "unauthorized" possession of something if he is not entitled to have it.

If you find that the accused's possession of (or control over or access to) the charged information was not unauthorized, you must find the accused not guilty.

Authority: Fifth Circuit: *United States v. Sink*, 586 F.2d 1041 (5th Cir. 1978), *cert. denied*, 443 U.S. 912 (1979). Tenth Circuit: *United States v. Zink*, 612 F.2d 511 (10th Cir. 1980).

(2) Information Related to National Defense:

The second element that the government must prove beyond a reasonable doubt is that the charged information is related to the national defense of the United States.

You must determine whether the charged information is directly and reasonably connected with the national defense. The term "national defense" is a broad term which refers to United States military and naval establishments and to all related activities of national preparedness. However, only information of the type which, if disclosed, could threaten the national security of the United States meets the definition of information "related to the national defense" for the purpose of this section. The connection must not be a strained one or an arbitrary one. The relationship must be reasonable and direct. Further, the type of harm that disclosure of the information is likely to cause must be endangerment to the environment of physical security which a functioning democracy requires. Finally, the Government must prove beyond a reasonable doubt that disclosure of the information would be likely to cause imminent serious injury to the United States. If the disclosure of this information does not pose this threat of imminent serious injury to the United States, then it is not information relating to the national defense.

Additionally, the Government must prove beyond a reasonable doubt that the Government closely held the information and that the accused knew the information was closely held. To do this, the Government must prove at least two things: (1) that the information was classified and (2) that the information was not otherwise available to the public. If, however, the information is lawfully accessible to anyone willing to take pains to find, to sift, and to collate it, you may not find the accused guilty of espionage under this section. Only information relating to our national defense which is not available to the public at the time of the claimed violation falls within the prohibition of this section.

If you find that the charged information is not related to the national defense of the United States, you must find the accused not guilty.

Authority: United States Supreme Court: *New York Times Co. v. United States*, 403 U.S. 713 (1971) (Brennan, J., concurring); *Gorin v. United States*, 312 U.S. 19 (1941). Second Circuit: *United States v. Soblen*, 301 F.2d 236 (2d Cir. 1962). Fourth Circuit: *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988); *United States v. Dedeyan*, 584 F.2d 36 (4th Cir. 1978); *United States v. Rosen*, 445 F. Supp. 2d 602 (E.D. Va. 2006).

(3) Information Could Be Used To Injury of the United States

The next element of the offense that the government must establish beyond a reasonable doubt is that the accused had reason to believe that the charged information could be used to the injury of the United States or to the advantage of any foreign nation.

"Reason to believe" means that the accused knew facts from which he concluded or reasonably should have concluded that the charged information could be used for the prohibited purposes. In considering whether or not the accused had reason to believe that the charged information could be used to the injury of the United States, or to the advantage of any foreign nation, you may consider the nature of the information involved.

Additionally, the likelihood of the information being used to the injury of the United States or to the advantage of any foreign nation must not be too remote, hypothetical, speculative, far-fetched or fanciful. Rather, the information must pose a legitimate danger of being used to the injury of the United States or to the advantage of any foreign nation, such that an accused knew or should have known about the information's capability to be used in this manner.

If you find that the accused did not have a reason to believe that the charged information could be used to the injury of the United States or to the advantage of any foreign nation, you must find the accused not guilty.

Authority: United States Supreme Court: *Gorin v. United States*, 312 U.S. 19 (1941). Fourth Circuit: *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979).

(4) Willfully Delivered Information to Person Not Entitled To Receive It

The next element of the offense that the government must establish beyond a reasonable doubt is that the accused willfully communicated (or delivered or transmitted or caused to be communicated, delivered, or transmitted or attempted to communicate, deliver, or transmit) the charged information to a [person or entity], who was not entitled to receive it.

In deciding whether the [person or entity] who received the charged information at issue was entitled to have it, you may consider all the evidence introduced at trial, including any evidence concerning the classification status of the document or testimony concerning limitations on

access to the document.

An act is done willfully if it is done voluntarily and intentionally and with the specific intent to do something the law forbids, that is to say, with a bad purpose either to disobey or disregard the law.

If you find that the accused's did not willfully communicated (*or delivered or transmitted or caused to be communicated, delivered, or transmitted or attempted to communicate, deliver, or transmit*) the charged information to a [person or entity], who was not entitled to receive it, you must find the accused not guilty.

Authority: Fourth Circuit: *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988). Ninth Circuit: *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979).

(5) Prejudicial to Good Order and Discipline and Service Discrediting Conduct

The final element of the offense which the government must establish beyond a reasonable doubt is that the accused's conduct was prejudicial to good order and discipline and of a nature to bring discredit upon the armed forces.

"Conduct prejudicial to good order and discipline" is conduct which causes a reasonable direct and obvious injury to good order and discipline. "Service discrediting conduct" is conduct which tends to harm the reputation of the service or lower it in public esteem.

If you find that the accused's conduct was not prejudicial to good order and discipline and/or was not of a nature to bring discredit upon the armed forces, you must find the accused not guilty.

Authority: Military Judges' Benchbook – notes under Article 134

2. The Defense respectfully requests the above instructions and definitions be given by the Court.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army,)

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

DEFENSE REQUESTED

INSTRUCTION:

**SPECIFICATIONS 4, 6, 8, 12 AND
16 OF CHARGE II**

DATED: 22 June 2012

1. The defense requests the following instructions to be given to the panel regarding Specifications 4, 6, 8, 12 and 16 of Charge II:

Court Instructions

In Specifications 4, 6, 8, 12 and 16 of Charge II, the accused is charged with the offense of stealing, purloining, or knowingly converting a thing of value of the United States, a violation of 18 U.S.C. Section 641. To find the accused guilty of this offense with regards to Specification 4, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

(1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: the Combined Information Data Network Exchange Iraq database containing more than 380,000 records, belonged to the United States government;

(2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 5 January 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;

(3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;

(4) That the value of the named property stolen, purloined, or knowingly converted was greater than \$1,000; and

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987).

Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 6, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: the Combined Information Data Network Exchange Afghanistan database containing more than 90,000 records, belonged to the United States government;
- (2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 8 January 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;
- (3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;
- (4) That the value of the named property stolen, purloined, or knowingly converted was greater than \$1,000; and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 8, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: a United States Southern Command database containing more than 700 records, belonged to the United States government;
- (2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, on or about 8 March 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;

- (3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;
- (4) That the value of the named property stolen, purloined, or knowingly converted was greater than \$1,000; and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 12, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: the Department of State Net-Centric Diplomacy database containing more than 250,000 records, belonged to the United States government;
- (2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 4 May 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;
- (3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;
- (4) That the value of the named property stolen, purloined, or knowingly converted was greater than \$1,000; and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S.

1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this offense with regards to Specification 16, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: the United States Forces – Iraq Microsoft Outlook/SharePoint Exchange Server global address list, belonged to the United States government;
- (2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 11 May 2010 and on or about 27 May 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;
- (3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;
- (4) That the value of the named property stolen, purloined, or knowingly converted was greater than \$1,000; and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

Court Definitions

(1) Money or Property Belonged to United States

The first element that the government must prove beyond a reasonable doubt is that the money or property alleged to have been stolen, purloined, or knowingly converted belonged to the United States government.

To satisfy this element, the government must prove that the named property was a “thing of value of the United States.” That means that at the time the property was allegedly stolen (or embezzled or knowingly converted) the United States government or an agency of the United States government had either title to, possession of, or control over, the property (or the property was made under contract for the United States).

If you find that the money or property was not a “thing of value of the United States,” you must find the accused not guilty.

Authority: 18 U.S.C. § 641. Second Circuit: *United States v. Girard*, 601 F.2d 69 (2d Cir.), *cert. denied*, 444 U.S. 871 (1979). Fourth Circuit: *United States v. Matzkin*, 14 F.3d 1014 (4th Cir. 1994). Sixth Circuit: *United States v. Barger*, 931 F.2d 359 (6th Cir. 1991). Seventh Circuit: *United States v. Croft*, 750 F.2d 1354 (7th Cir. 1984). Eighth Circuit: *United States v. Wilson*, 636 F.2d 225 (8th Cir. 1980). District of Columbia Circuit: *United States v. Collins*, 56 F.3d 1416 (D.C. Cir. 1995) (per curiam).

(2) Accused Stole, Purloined or Knowingly Converted Property

The second element that the government must prove beyond a reasonable doubt is that the accused stole (or purloined or knowingly converted) the property of the United States government.

[If stealing is charged]: To steal money or property means to take someone else’s money or property without the owner’s consent with the intent to deprive the owner of the value of that money or property.

[If purloined is charged]: To purloin is to steal with the element of stealth, that is, to take by stealth someone else’s property without the owner’s consent with the intent to permanently deprive the owner of the value of that property.

[If conversion is charged]: To knowingly convert property means to exercise control over the property in an unauthorized manner in a way which seriously or substantially interferes with the government’s right to use and control its own property, knowing that the property belonged to the United States, and knowing that such use was unauthorized. Mere misuse of the property is not enough for you to find that the accused knowingly converted it. Rather, you must find that such misuse seriously or substantially interfered with the government’s ownership rights in that property.

If you find that the accused did not steal (or purloin or knowingly convert) the money or property, you must find the accused not guilty.

Authority: United States Supreme Court: *Morissette v. United States*, 342 U.S. 246 (1952). Third Circuit: *United States v. Oliver*, 238 F.3d 471 (3d Cir. 2001). Fourth Circuit: *United States v. Maisel*, 12 F.3d 423 (4th Cir. 1993); *United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991); *United States v. Fogel*, 901 F.2d 23 (4th Cir.), *cert. denied*, 498 U.S. 939 (1990). Fifth Circuit: *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992). Eighth Circuit: *United States v. May*, 625 F.2d 186 (8th Cir. 1980). Ninth Circuit: *United States v. Thordarson*, 646 F.2d 1323 (9th Cir. 1981). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). District of Columbia Circuit: *United States v. Collins*, 56 F.3d 1416 (D.C. Cir. 1995) (per curiam).

(3) Intent

The third element that the government must prove beyond a reasonable doubt is that the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property.

To act knowingly means to act intentionally and voluntarily, and not because of ignorance, mistake, accident or carelessness.

To act willfully means to act with knowledge that one's conduct is unlawful and with the intent to do something that the law forbids, that is to say, with the bad purpose to disobey or disregard the law.

Whether the accused acted knowingly and willfully may be proven by the accused's conduct and by all of the circumstances surrounding the case.

If you find that the accused did not act knowingly and willfully with the intent to deprive the government of the use and benefit of its property, you must find the accused not guilty.

Authority: United States Supreme Court: *Morissette v. United States*, 342 U.S. 246 (1952). Fourth Circuit: *United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991). Fifth Circuit: *United States v. Shackelford*, 677 F.2d 422 (5th Cir. 1982), *cert. denied*, 494 U.S. 899 (1983). Seventh Circuit: *United States v. Croft*, 750 F.2d 1354 (7th Cir. 1984). Eighth Circuit: *United States v. Wilson*, 636 F.2d 225 (8th Cir. 1980). Ninth Circuit: *United States v. Scott*, 789 F.2d 795 (9th Cir. 1986); *United States v. Eden*, 659 F.2d 1376 (9th Cir. 1981), *cert. denied*, 455 U.S. 949 (1982). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); *United States v. Burton*, 871 F.2d 1566 (11th Cir. 1989).

(4) Value of Property

The fourth element which the government must prove beyond a reasonable doubt is that the value of the property allegedly stolen, purloined, or knowingly converted was greater than \$1,000.

The word "value" means face, par or market value, or cost price, either wholesale or retail, whichever is greater. "Market value" means the price a willing buyer would pay a willing seller at the time the property was stolen, purloined, or knowingly converted. "Cost price" means the cost of producing or creating the specific property allegedly stolen, purloined, or knowingly converted.

Whichever method of proving value the Government chooses to pursue, you are not permitted to infer the requisite value merely from your common knowledge or experience. Rather, the Government must put forth evidence to prove to you beyond a reasonable doubt that the value of the specific property allegedly stolen, purloined, or knowingly converted exceeded \$1,000.

If you find that the aggregate value is \$1,000 or less, then you must find the accused not guilty.

Authority: Third Circuit: *United States v. DiGilio*, 538 F.2d 972 (3d Cir. 1976), *cert. denied sub nom.*, *Lupo v. United States*, 429 U.S. 1038 (1977). Fourth Circuit: *United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991); *United States v. Wilson*, 284 F.2d 407 (4th Cir. 1960). Sixth Circuit: *United States v. Jeter*, 775 F.2d 670 (6th Cir. 1985), *cert. denied*, 475 U.S. 1142 (1986). Seventh Circuit: *United States v. Oberhardt*, 887 F.2d 790 (7th Cir. 1989). Eighth Circuit: *United States v. May*, 625 F.2d 186 (8th Cir. 1980). Ninth Circuit: *United States v. Sargent*, 504 F.3d 767 (9th Cir. 2007).

(5) Prejudicial to Good Order and Discipline and Service Discrediting Conduct

The final element of the offense which the government must establish beyond a reasonable doubt is that the accused's conduct was prejudicial to good order and discipline and of a nature to bring discredit upon the armed forces.

"Conduct prejudicial to good order and discipline" is conduct which causes a reasonable direct and obvious injury to good order and discipline. "Service discrediting conduct" is conduct which tends to harm the reputation of the service or lower it in public esteem.

If you find that the accused's conduct was not prejudicial to good order and discipline and/or was not of a nature to bring discredit upon the armed forces, you must find the accused not guilty.

Authority: Military Judges' Benchbook – notes under Article 134

2. Additionally, as a lesser-included offense (LIO) for each of the Section 641 offenses alleged in Specifications 4, 6, 8, 12 and 16 of Charge II, the Defense requests the following instructions:

Court LIO Instructions

In Specifications 4, 6, 8, 12 and 16 of Charge II, the accused is charged with the offense of stealing, purloining, or knowingly converting a thing of value of the United States, a violation of 18 U.S.C. Section 641. If, for any of these offenses, you find that the Government has not proved beyond a reasonable doubt that the property in question had a value in excess of \$1,000, you may consider whether the accused is guilty of the lesser-included offense of stealing, purloining, or knowingly converted a thing of value of the United States not having a value in excess of \$1,000, a violation of 18 U.S.C. Section 641.

To find the accused guilty of this lesser-included offense with regards to Specification 4, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

(1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: the Combined Information Data Network Exchange Iraq database containing more than 380,000 records, belonged to the United States government;

(2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 5 January 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;

(3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;

(4) That the named property stolen, purloined, or knowingly converted had some value of \$1,000 or less; and

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 641. Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this lesser-included offense with regards to Specification 6, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

(1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: the Combined Information Data Network Exchange Afghanistan database containing more than 90,000 records, belonged to the United States government;

(2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 8 January 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;

(3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;

(4) That the named property stolen, purloined, or knowingly converted had some value of \$1,000 or less; and

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 641. Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal

Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this lesser-included offense with regards to Specification 8, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: a United States Southern Command database containing more than 700 records, belonged to the United States government;
- (2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, on or about 8 March 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;
- (3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;
- (4) That the named property stolen, purloined, or knowingly converted had some value of \$1,000 or less; and
- (5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 641. Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this lesser-included offense with regards to Specification 12, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

- (1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: the Department of State Net-Centric Diplomacy database containing more than 250,000 records, belonged to the United States government;

(2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 4 May 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;

(3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;

(4) That the named property stolen, purloined, or knowingly converted had some value of \$1,000 or less; and

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: 18 U.S.C. § 641. Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

Similarly, to find the accused guilty of this lesser-included offense with regards to Specification 16, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

(1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: the United States Forces – Iraq Microsoft Outlook/SharePoint Exchange Server global address list, belonged to the United States government;

(2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 11 May 2010 and on or about 27 May 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;

(3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property;

(4) That the named property stolen, purloined, or knowingly converted had some value of \$1,000 or less; and

(5) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.¹

Authority: Fifth Circuit: *United States v. Dien Duc Huynh*, 246 F.3d 734 (5th Cir. 2001); *United States v. Aguilar*, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33. Seventh Circuit: *United States v. Howard*, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641. Eighth Circuit: Eighth Circuit Model Criminal Jury Instruction 6.18.641. Ninth Circuit: *United States v. Seaman*, 18 F.3d 649 (9th Cir. 1994). Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987). Eleventh Circuit: *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21; Military Judges Benchbook, DA Pam 27-9.

3. The Defense respectfully requests the above instructions and definitions be given by the Court.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

¹ For the more detailed instructions on each of the elements of this LIO, the Defense relies on those provided *supra* at 4-7, except that the language in the instruction for the value element should be changed to reflect some value of \$1,000 or less.

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, [REDACTED])

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

DEFENSE REQUESTED

INSTRUCTION: ARTICLE 104

DATED: 22 June 2012

1. The defense requests the following instructions to be given to the panel regarding the Specification of Charge 1:

Court Instructions

In the Specification and Charge I, the accused is charged with the offense of Aiding the Enemy, a violation of Article 104, UCMJ. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following four (4) elements:

- (1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, without proper authority, knowingly gave intelligence information to the enemy, namely: Al-Qaida, Al-Qaida in the Arabian Peninsula, and an entity specified in Bates Number 00410660 through 00410664;
- (2) That the accused did so by indirect means;
- (3) That Al-Qaida, Al-Qaida in the Arabian Peninsula, and an entity specified in Bates Number 00410660 through 00410664 was an enemy; and
- (4) That this intelligence information is true, at least in part.

Authority: Article 104(2), UCMJ, 10 U.S.C. § 904(2); Military Judges Benchbook, DA Pam 27-9, para. 3-28-4.

Court Definitions

(1) Knowingly Gave Intelligence Information to the Enemy

The first element which the government must prove beyond a reasonable doubt is that the accused, without proper authority, knowingly gave intelligence to the enemy and that he knew at the time that the individuals that he gave the intelligence to were enemies of the United States.

In order to find the accused guilty of giving intelligence to the enemy through indirect means, you must be convinced beyond a reasonable doubt that the accused had actual knowledge that he was giving intelligence to the enemy through the indirect means. An accused has actual knowledge that he is giving intelligence to the enemy through indirect means only when he knowingly and intentionally provides intelligence to the enemy through the indirect means. Providing intelligence to a third party with reason to believe that the enemy might receive it, could receive it, or even would likely receive it, is insufficient. Rather, you must be convinced beyond a reasonable doubt that the accused, using the third party as a mere conduit, knowingly and intentionally gave intelligence to the enemy. That is, the accused must have used the third party for the purpose of giving the intelligence to the enemy.

If you find that the accused honestly believed that he was giving intelligence only to a third party and that he was not giving it to the enemy, you must find the accused not guilty of the offense of giving intelligence to the enemy through indirect means.

Authority: Article 104(2), UCMJ, 10 U.S.C. § 904(2); *United States v. Anderson*, 68 M.J. 378, 387 (C.A.A.F. 2010); *United States v. Batchelor*, 22 C.M.R. 144, 156-159 (C.M.A. 1956); *United States v. Olson*, 20 C.M.R. 461, 464 (A.B.R. 1955).

(2) Indirect Means

The second element which the government must prove beyond a reasonable doubt is that the accused gave the intelligence to the enemy through indirect means.

The term “indirect” is intended to reach the usage of intermediaries for the purpose of conveying information to the enemy. The Government must prove that the accused had the general intent to use an intermediary to provide the information to the enemy and that the accused actually knew that by giving information to the intermediary he was giving the intelligence to the enemy. Absent an intention that the intermediary convey the information to the enemy, the accused’s communication with a non-enemy individual or entity is not an “indirect” communication with the enemy regardless of whether an enemy ultimately was able to receive the substance of the information that the accused provided to the non-enemy.

If you find that the government failed to prove beyond a reasonable doubt that the accused intended to use an intermediary to convey the intelligence to the enemy, then you must find the accused not guilty.

Authority: Article 104(2), UCMJ, 10 U.S.C. § 904(2); *United States v. Anderson*, 68 M.J. 378, 387 (C.A.A.F. 2010); *United States v. Batchelor*, 22 C.M.R. 144, 156-159 (C.M.A. 1956).

(3) Enemy

The third element which the government must prove beyond a reasonable doubt is that the entity that received the information was an enemy.

"Enemy" includes (not only) organized opposing forces in time of war, (but also any other hostile body that our forces may be opposing) (such as a rebellious mob or a band of renegades) (and includes civilians as well as members of military organizations). ("Enemy" is not restricted to the enemy government or its armed forces. All the citizens of one belligerent are enemies of the government and the citizens of the other.)

If you find that the government failed to prove beyond a reasonable doubt that the entity that the accused intended to provide the information to, either directly or indirectly, was an enemy, then you must find the accused not guilty.

Authority: Article 104(2), UCMJ, 10 U.S.C. § 904(2); Military Judges' Benchbook, DA Pam 27-9, para. 3-28-4.

(4) Intelligence Information Was True

The fourth element which the government must prove beyond a reasonable doubt is that the intelligence information was true, at least in part. "Intelligence" means any helpful information, given to and received by the enemy, which is true, at least in part.

If you find that the government failed to prove beyond a reasonable doubt that the information that that the accused intended to provide was true, at least in part, then you must find the accused not guilty.

Authority: Article 104(2), UCMJ, 10 U.S.C. § 904(2); Military Judges' Benchbook, DA Pam 27-9, para. 3-28-4.

2. The Defense respectfully requests the above instructions and definitions be given by the Court.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of conduct prejudicial to good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, UCMJ, 10 U.S.C. §§ 892, 904, 934 (2010).

4. Specifically, the Specification of Charge I alleges that PFC Manning “did, at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, without proper authority, knowingly give intelligence to the enemy, through indirect means[.]” in violation of Article 104. *See* Charge Sheet. The Defense, in its Motion for a Bill of Particulars, asked the Government to specify the indirect means allegedly used by PFC Manning to give this intelligence to the enemy. “The Government responded ‘PFC Manning knowingly gave intelligence to the enemy by transmitting certain intelligence, specified in a separate classified document, to the enemy through the WikiLeaks website.’” Appellate Exhibit LXXXI, at 1 (quoting Government Response to Defense Motion for a Bill of Particulars). The Government has further clarified that the “enemy” to whom PFC Manning allegedly indirectly gave intelligence is Al-Qaida, Al-Qaida in the Arabian Peninsula, and an entity specified in Bates Number 00410660 through 00410664.

5. On 26 April 2012, this Court denied the Defense Motion to Dismiss the Specification of Charge I for Failure to State an Offense. *See* Appellate Exhibit LXXXI, at 5. In that decision, this Court held that “Giving Intelligence to the Enemy under Article 104(2) requires *actual knowledge* by the accused that he was giving intelligence *to the enemy*.” *Id.* at 2 (emphases supplied). This Court also invited the parties to propose instructions for the “knowledge” and “indirect means” elements of the violation of Article 104 charged in the Specification of Charge I. *See id.* at 4. This motion sets forth the Defense’s proposed instructions for the “knowledge” element of that offense.¹

WITNESSES/EVIDENCE

6. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the following evidence in support of the Defense’s motion:

- a. Charge Sheet;
- b. Attachment A, Manual for Military Commissions (MMC) excerpt; and
- c. Attachment B, Military Commissions Act of 2009 excerpt.

¹ In regards to the other elements of the violation of Article 104 charged in the Specification of Charge I, including the “indirect means” element, the Defense relies on the Defense Requested Instruction: Article 104.

LEGAL AUTHORITY AND ARGUMENT

7. As this Court has held, an accused must have *actual knowledge* that he is giving intelligence to the enemy in order to be convicted of a violation of Article 104(2). See Appellate Exhibit LXXXI, at 2. This actual knowledge element is an essential element of a violation of Article 104(2), regardless of whether that violation involves directly or indirectly giving intelligence to the enemy. See *id.* In light of this Court's ruling, the Defense proposes that the Court instruct the members that where, as here, the accused is charged with indirectly giving intelligence to the enemy, this actual knowledge element requires the Government to prove beyond a reasonable doubt that the accused, using the third party as a mere conduit, knowingly and intentionally gave intelligence information to the enemy. In other words, the Government must prove that the accused used the third party for the purpose of giving intelligence information to the enemy.

8. This instruction on the actual knowledge element is most consistent with the case law interpreting Article 104(2), including this Court's 26 April 2012 decision. Additionally, it is supported by both Offense 26 of the Military Commissions Act, see 10 U.S.C. § 950t(26), and the common law of war.

9. Therefore, the Defense requests this Court to adopt its proposed instruction on the actual knowledge element.

A. A "Knowingly and Intentionally" Requirement is Consistent With the Case Law Interpreting Article 104(2)

10. Defining the actual knowledge element to require the Government to prove beyond a reasonable doubt that the accused, using the third party as a mere conduit, knowingly and intentionally gave intelligence information to the enemy is the definition that is most consistent with the case law interpreting Article 104(2), including this Court's 26 April 2012 ruling. Moreover, any watered-down instruction on actual knowledge that would, for instance, be satisfied where the accused merely had knowledge that intelligence given to a third party might be received by the enemy, could be received by the enemy, or even would likely be received by the enemy, would impermissibly turn Article 104(2) into a strict liability offense.

11. Article 104(2) punishes "[a]ny person who . . . (2) without proper authority, knowingly harbors or protects or gives intelligence to, or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly." 10 U.S.C. § 904. The Manual for Courts-Martial (MCM) explains that the textual requirement that an accused "knowingly . . . gives intelligence" requires the accused to have actual knowledge that he is giving intelligence to the enemy. See MCM, Part IV, para. 28.c(5)(c) ("Actual knowledge is required but may be proved by circumstantial evidence.").

12. Case law interpreting Article 104(2) makes clear that mere knowledge that the enemy might receive the intelligence, or could receive the intelligence, or even would likely receive the intelligence is insufficient to satisfy the actual knowledge requirement. Courts have uniformly

held that the Government must prove that the accused knowingly and intentionally gave intelligence to the enemy under Article 104(2). *See United States v. Anderson*, 68 M.J. 378, 387 (C.A.A.F. 2010); *United States v. Batchelor*, 22 C.M.R. 144, 157 (C.M.A. 1956); *United States v. Olson*, 20 C.M.R. 461, 464 (A.B.R. 1955).

13. In *Olson*, for example, the United States Army Board of Review held that Article 104 “does require a general evil intent in order to protect the innocent who may commit some act in aiding the enemy inadvertently, accidentally, or negligently.” 20 C.M.R. at 464. Similarly, in *Batchelor*, the Court of Military Appeals explained that there was “no doubt that [defense] counsel are on sound ground when they assert that [Article 104] requires a showing of criminal intent, and the Government concedes that premise to be true . . . [S]urely an offense which is so closely akin to treason and may be punished by a death sentence cannot be viewed as a ‘public welfare’ kind of dereliction.” 22 C.M.R. at 157. Rather, the Court observed that proper instructions for an Article 104 offense must require “the finding of general criminal intent.” *Id.* at 158. Finally, the Court of Appeals for the Armed Forces in *Anderson*, by comparing Article 104 with an offense charged under Article 134, emphasized that an accused’s intent behind the conduct at issue matters in an Article 104 prosecution: “Unlike Article 104, UCMJ, the general offense as charged [as a violation of Article 134] prohibits the dissemination of the information regardless of the intent behind that dissemination.” 68 M.J. at 387 (emphases supplied).

14. Additionally, this Court’s 26 April 2012 ruling provides further support that the actual knowledge element of an Article 104(2) prosecution requires proof that the accused knowingly and intentionally gave intelligence to the enemy. In that ruling, after holding that Article 104(2) requires that the accused had actual knowledge that he was giving intelligence to the enemy, this Court proposed the following instruction for knowledge:

Knowingly means Giving Intelligence to the Enemy under Article 104(2) requires *actual knowledge* by the accused that he was giving intelligence to the enemy. This is true whether the giving of intelligence is by direct or indirect means. A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently. *See* MCM, Paragraph 28c(5)(c). *U.S. v. Olson*, 20 C.M.R. 461 (A.B.R. 1955).

Appellate Exhibit LXXX1, at 4 (emphases supplied). This instruction demonstrates that the act of giving the intelligence to the enemy must be knowing and intentional; it cannot be an inadvertent mistake, accident or negligent act. *See id.* This Court’s proposed definition of “indirect means” further bolsters the conclusion that an accused must knowingly and intentionally give intelligence to the enemy. This Court proposed the following definition of “indirect means:”

“Indirect means” means that the accused knowingly gave intelligence to the enemy through a 3rd party or in some other indirect way. The accused must actually know that by giving intelligence to the 3rd party he was giving intelligence to the enemy through this indirect means.

Id. (emphasis supplied). Since “[t]he accused must actually know that by giving intelligence to the 3rd party he was giving intelligence to the enemy through this indirect means[.]” *id.*, an accused cannot be found guilty of giving intelligence to the enemy where he gives intelligence to a third party with the mere knowledge that the enemy might, could, or even would likely receive the intelligence. Rather, the instruction properly requires that an accused, using the third party as a conduit, knowingly and intentionally gives intelligence to the enemy.

15. Indeed, permitting an Article 104(2) conviction where the accused gave intelligence to a third party with the mere knowledge that the enemy might, could, or even would likely receive the intelligence would convert Article 104(2) into a strict liability offense. Today, everyone understands that information posted on a publicly accessible website can potentially be viewed by anyone with Internet access. See *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 851 (1997) (“Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail (e-mail), automatic mailing list services (‘mail exploders,’ sometimes referred to as ‘listservs’), ‘newsgroups,’ ‘chat rooms,’ and the ‘World Wide Web.’ All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium – known to its users as ‘cyberspace’ – located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.”).

16. Therefore, if the actual knowledge element of Article 104(2) only encompasses something less than knowingly and intentionally giving intelligence to the enemy, then the actual knowledge element would be satisfied in any case where anyone subject to the UCMJ causes intelligence to be published on the Internet since everyone knows that anyone with Internet access, including the enemy, could obtain information placed on the Internet. See *Reno*, 521 U.S. at 851. Not only does this result render the actual knowledge element of Article 104(2) identified by this Court in its 26 April 2012 ruling utterly toothless in all Internet-intelligence cases, it transforms Article 104 into a strict liability offense, punishing anyone who causes intelligence to be published on the internet, regardless of whether that act intentionally, inadvertently, accidentally, or negligently gave intelligence to the enemy. Binding precedent from the highest military court clearly forecloses such an expansive use of Article 104. See *Batchelor*, 22 C.M.R. at 157 (“[S]urely an offense which is so closely akin to treason and may be punished by a death sentence cannot be viewed as a ‘public welfare’ kind of dereliction.”); see also *Olson* 20 C.M.R. at 464 (holding that Article 104 “does require a general evil intent in order to protect the innocent who may commit some act in aiding the enemy inadvertently, accidentally, or negligently”); Court’s Ruling - Appellate Exhibit LXXXI, at 2, 4 (“A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently.”).

17. Simply put, one cannot knowingly give intelligence to the enemy without intentionally giving the intelligence to the enemy. If one knowingly performs an act (e.g. giving intelligence to the enemy through indirect means), he intentionally performs that act. For instance, if a Soldier is charged with arson and the mens rea for that offense is that the defendant “knowingly set fire,” “knowingly” is equivalent to “intentionally” (i.e. intentionally set something on fire). Even though the Government need not prove that the Soldier intended the further consequences

of his act – that is, to burn down a building – the Government still must prove that the Soldier intended the initial actus reus. Cf. *Morissette v. United States*, 342 U.S. 246, 270-71 (1952) (explaining, when discussing the offense of knowing conversion of government property, that “knowing conversion requires more than knowledge that defendant was taking the property into his possession. He must have had knowledge of the facts, though not necessarily the law, that made the taking a conversion. In the case before us, whether the mental element that Congress required be spoken of as knowledge or as intent, would not seem to alter its bearing on guilt[.] for it is not apparent how Morissette could have knowingly or intentionally converted property that he did not know could be converted, as would be the case if it was in fact abandoned or if he truly believed it to be abandoned and unwanted property.”). The same can be said for knowingly giving intelligence to the enemy: whenever an accused, using a third party as a mere conduit, knowingly gives intelligence to the enemy, he must, of necessity, also intentionally give the intelligence to the enemy through the same indirect means.² Including the “knowingly and intentionally” requirement in the actual knowledge element is simply a way to ensure that an accused is not convicted because he has knowledge that an enemy *might, could, or even would likely* receive the intelligence. If any of these loose conceptions of knowledge is the standard adopted by the Court, Article 104(2) would punish giving intelligence to the enemy “inadvertently, accidentally, or negligently.” *Olson*, 20 C.M.R. at 464. Well-established Article 104 precedent, including this Court’s 26 April 2012 decision, plainly forbids this result. See *Anderson*, 68 M.J. at 387; *Batchelor*, 22 C.M.R. at 157; *Olson*, 20 C.M.R. at 464; see also Appellate Exhibit LXXXI, at 2, 4 (“A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently.”).

18. Therefore, this Court should adopt in full the Defense’s proposed instruction and instruct the members that where, as here, the accused is charged with indirectly giving intelligence to the enemy, the actual knowledge element requires the Government to prove beyond a reasonable doubt that the accused, using the third party as a mere conduit, knowingly and intentionally gave intelligence information to the enemy.

B. A “Knowingly and Intentionally” Requirement is Supported by Offense 26 of the Military Commissions Act and by the Common Law of War

19. Offense 26 of the Military Commissions Act and the common law of war further support the conclusion that the actual knowledge element of an Article 104(2) prosecution requires the Government to prove that the accused knowingly and intentionally gave intelligence to the enemy.

20. Offense 26 of the Military Commissions Act, entitled “Wrongfully aiding the enemy” (Offense 26), provides in full as follows:

² Saying that an accused acted “intentionally” in this context is not the same as saying an accused acted with any type of specific intent or motive (e.g. intent to aid the enemy). See Appellate Exhibit LXXXI, at 3. Rather, the term “intentionally” here simply means that the accused intended to perform the act (i.e. intended to give intelligence to the enemy). In other words, it means that he did not act “inadvertently, accidentally, or negligently.” *Olson*, 20 C.M.R. at 464; see Appellate Exhibit LXXXI, at 2, 4 (“A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently.”)

Any person subject to this chapter who, in breach of an allegiance or duty to the United States, *knowingly and intentionally* aids an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished as a military commission under this chapter may direct.

10 U.S.C. § 950t(26) (emphasis supplied); *see also* Attachment A, Manual for Military Commissions (MMC), Part IV, at 20-21 (2010 ed.) (containing this language). A comparison of the statutory text of Offense 26 and Article 104, as well as an examination of the legislative history of the Military Commissions Act, demonstrates that Offense 26 was directly patterned after Article 104.

21. Offense 26 prohibits several acts punished by Article 104, including giving intelligence to the enemy. *Compare* 10 U.S.C. § 104 (punishing “[a]ny person who – (1) aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other things; or (2) without proper authority, knowingly harbors or protects or *gives intelligence to*, or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly”) (emphasis supplied)), *with* MMC, Part IV, at 21 (“The means the accused can use to aid the enemy include but are not limited to: providing arms, ammunition, supplies, money, or other items or services to the enemy; harboring or protecting the enemy; or *giving intelligence or other information to the enemy.*” (emphasis supplied)). Indeed, all forms of aiding the enemy prohibited by Offense 26 are also prohibited by Article 104.

22. The statutory text now contained in Section 950t(26) was supplied by the Military Commissions Act of 2009. *See* Attachment B, Military Commissions Act of 2009, Pub. L. No. 111-84, tit. 18, § 1802, 123 Stat. 2190, 2611 (codified at 10 U.S.C. §§ 948a–950t). The language of Offense 26 in Section 950t(26) replaced identical language in the Military Commissions Act of 2006, which was contained in 10 U.S.C. Section 950v(b)(26). *See* 10 U.S.C. § 950v(b)(26) (2006) (containing language identical to that contained in Section 950t(26)). The Report of the House Committee on Armed Services accompanying the Military Commissions Act of 2006 indicated that the offenses listed in then-Section 950v(b) (now Section 950t) were not new offenses, but were rather modern war crimes or offenses triable by military commissions or international courts:

[T]he committee believes the list [of offenses in 10 U.S.C. Section 950v(b)] codifies offenses hitherto recognized as offenses triable by military commissions or international courts. Most of the listed offenses constitute clear violations of the Geneva Conventions, the Hague Convention, or both. Several constitute “modern-day war crimes,” such as hijacking and terrorism, which constitute practices contrary to the law of nations that can, and hereby do, have the same status as traditional war crimes.

H.R. Rep. No. 109-664, pt. 1, at 28 (2006).

23. Moreover, Section 950p(d) makes clear that the offenses currently listed in Section 950t, including Offense 26, are not new offenses, but are instead codifications of offenses traditionally triable by military commission. *See* 10 U.S.C. § 950p(d) (“The provisions of this subchapter

codify offenses that have traditionally been triable by military commission. This chapter does not establish new crimes that did not exist before the date of the enactment of this subchapter[.]”).

24. Therefore, the close similarity between Offense 26 and Article 104, when coupled with the fact that Offense 26, like all offenses listed in Section 950t, is not a new offense but simply a codification of an existing offense, leads to the inescapable conclusion that Offense 26 was directly patterned after Article 104.

25. Offense 26 requires an accused to knowingly and intentionally aid the enemy. See 10 U.S.C. § 950t(26); see also MMC, Part IV, at 21 (listing the following as the second element of Offense 26: “The accused intended to aid the enemy.”). Since Offense 26 is not a new offense, see 10 U.S.C. § 950p(d), and is obviously patterned after Article 104, this requirement that an accused knowingly and intentionally aid the enemy must come from Article 104. Accordingly, where, as here, the accused is alleged to have aided the enemy by giving intelligence to the enemy, see MCM, Part IV, para. 28.c(5)(a) (“Giving intelligence to the enemy is a particular case of corresponding with the enemy made more serious by the fact that the communication contains intelligence that may be useful to the enemy for any of the many reasons that make information valuable to belligerents”), Article 104 requires that the accused knowingly and intentionally give the intelligence to the enemy.

26. If Article 104 does not require an accused to knowingly and intentionally give intelligence to the enemy, a very troublesome absurdity would exist. In a prosecution of a terrorist under Offense 26, the Government would be required to prove that the terrorist knowingly *and intentionally* aided the enemy. Yet in a prosecution of a Soldier under Article 104 for giving intelligence to the enemy, the Government would only be required to prove that the Soldier knowingly gave intelligence to the enemy. Thus, for the exact same conduct, a terrorist would benefit from a friendlier mens rea than a Soldier would. Congress could not have intended to give terrorists a more protective mens rea than it gave to Soldiers. It defies all logic to think that a terrorist would fare better in an American court for aiding the enemy than a U.S. soldier would. To make sense of this all, Article 104, like Offense 26, must require the Government to prove that the accused knowingly *and intentionally* gave intelligence to the enemy.

27. Additionally, aiding the enemy by giving intelligence to the enemy is one of the “common law” war crimes. The Government has recently explained this point in its briefing in another case. See Brief for Respondent United States at 41-45, *Hamdan v. United States*, No. 11-1257 (D.C. Cir. Jan. 17, 2012). In its brief before the District of Columbia Circuit in *Hamdan*, the Government explained that “[s]ince the adoption of the Constitution, Congress and the Executive have repeatedly employed their war-making powers to identify . . . ‘common law’ war crimes and to make those offenses triable by military tribunal, rather than by an Article III Court.” *Id.* at 41. The Government then identified aiding the enemy as one of these “common law” war crimes. *Id.* at 44 (explaining that “aiding the enemy (by someone with a duty of loyalty to the United States), although not a war crime under international law, has long constituted an offense under the U.S. law of war, making the offender subject to trial by military tribunal.”). The Government identified the Articles of War of 1775 as the first American military law to punish aiding the enemy and from there concluded that “[t]his prohibition on aiding the enemy has

remained substantially the same during the past 235 years.” *Id.*; see also *id.* at 44-45 n.15 (citing various provisions punishing aiding the enemy over the years, including Article 104).

28. The Government then observed that:

[b]oth aiding the enemy in violation of a duty of loyalty and spying [which the Government also identified as constituting a “common law” war crime] are offenses subject to trial by military commission under the 2006 and 2009 [Military Commissions Acts], and both are offenses that constitute . . . this nation’s “common law of war.”

Id. at 45 (footnote omitted); see also *id.* at 45 n.16 (citing 10 U.S.C. § 950t(26) and 10 U.S.C. § 950v(b)(26)). Offense 26, codified at Section 950t(26), thus represents the most recent installment of the common law of war offense of aiding the enemy which “has remained substantially the same during the past 235 years.” *Id.* at 44. As mentioned above, Offense 26 does not create a new offense in any way. See 10 U.S.C. § 950p(d). Therefore, it is simply a present restatement of the common law of war offense of aiding the enemy. As Offense 26 contains a requirement that the accused knowingly and intentionally aid the enemy, that knowingly and intentionally requirement must come from the common law of war offense, unchanged for 235 years. Because Article 104 represents the modern version of this common law of war offense, it too must include the knowingly and intentionally requirement for the offense of giving intelligence to the enemy.

29. Therefore, Offense 26 and the common law of war provide further evidence that the Defense instruction, requiring as it does that the Government prove that the accused knowingly and intentionally gave intelligence to the enemy through indirect means, is correct and should be adopted in full by this Court.

CONCLUSION

30. For the reasons articulated above, the Defense requests that this Court give the following instruction to the members on the “knowingly” element of the Specification of Charge I:

“In order to find the accused guilty of giving intelligence to the enemy through indirect means, you must be convinced beyond a reasonable doubt that the accused had actual knowledge that he was giving intelligence to the enemy through the indirect means. An accused has actual knowledge that he is giving intelligence to the enemy only when he knowingly and intentionally provides intelligence to the enemy through the indirect means. Providing intelligence to a third party with reason to believe that the enemy might receive it, could receive it, or even would likely receive it, is insufficient. Rather, you must be convinced beyond a reasonable doubt that the accused, using the third party as a mere conduit, knowingly and intentionally gave intelligence to the enemy. That is, the accused must have used the third party for the purpose of giving the intelligence to the enemy. If you find that the accused honestly believed that he was giving intelligence only to a third party and that he was not giving it to the enemy, you must find

the accused not guilty of the offense of giving intelligence to the enemy through indirect means."³

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

³ This last sentence of the Defense's proposed instruction is simply a necessary consequence of this Court's finding that the accused must have actual knowledge that he is giving intelligence to the enemy. Where an offense requires actual knowledge as to some fact (e.g. actual knowledge that an accused was giving intelligence to the enemy), an honest mistake as to that fact -- without regard to the reasonableness of the mistake -- is a complete defense to the offense. See *United States v. Nix*, 29 C.M.R. 507, 511 (C.M.A. 1960); *United States v. Walters*, 28 C.M.R. 164, 167 (C.M.A. 1959) ("[W]here subjective knowledge is required, reasonableness is not one of the criteria which should be used in instructing on mistake of law or fact.").

ATTACHMENT A

MANUAL FOR MILITARY COMMISSIONS

UNITED STATES

(2010 EDITION)

Table of Contents – Manual for Military Commissions

c. Comment.	IV-19
d. Maximum punishment.	IV-19
(24) TERRORISM	IV-19
a. Text.	IV-19
b. Elements.	IV-19
c. Comment.	IV-19
d. Maximum Punishment.	IV-20
(25) PROVIDING MATERIAL SUPPORT FOR TERRORISM	IV-20
a. Text.	IV-20
b. Elements.	IV-20
c. Definition.	IV-20
d. Maximum Punishment.	IV-20
(26) WRONGFULLY AIDING THE ENEMY	IV-20
a. Text.	IV-20
b. Elements	IV-21
c. Comment.	IV-21
d. Maximum punishment	IV-21
(27) SPYING	IV-21
a. Text	IV-21
b. Elements	IV-21
c. Comment	IV-22
d. Maximum punishment	IV-22
(28) ATTEMPTS	IV-22
a. Text	IV-22
b. Elements.	IV-22
c. Maximum punishment.	IV-23
(29) CONSPIRACY	IV-23
a. Text	IV-23
b. Elements.	IV-23
c. Comment.	IV-23
d. Maximum Punishment.	IV-24
(30) SOLICITATION.	IV-24
a. Text.	IV-24
b. Elements.	IV-24
c. Maximum punishment.	IV-25
(31) CONTEMPT.	IV-25
a. Text.	IV-25

d. *Maximum Punishment.* Death, if the death of any person occurs as a result of the terrorist act. Otherwise, confinement for life.

(25) PROVIDING MATERIAL SUPPORT FOR TERRORISM.

a. *Text.* "Any person subject to this chapter who provides material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, an act of terrorism (as set forth in paragraph (24) of this section), or who intentionally provides material support or resources to an international terrorist organization engaged in hostilities against the United States, knowing that such organization has engaged or engages in terrorism (as so set forth), shall be punished as a military commission under this chapter may direct."

b. *Elements.* The elements of this offense can be met either by meeting (i) all of the elements in A, or (ii) all of the elements in B, or (iii) all of the elements in both A and B:

A. (1) The accused provided material support or resources to be used in preparation for, or in carrying out, an act of terrorism (as set forth in paragraph (24));

(2) The accused knew or intended that the material support or resources were to be used for those purposes; and

(3) The conduct took place in the context of and was associated with an hostilities.

B. (1) The accused provided material support or resources to an international terrorist organization engaged in hostilities against the United States;

(2) The accused intended to provide such material support or resources to such an international terrorist organization;

(3) The accused knew that such organization has engaged or engages in terrorism; and

(4) The conduct took place in the context of and was associated with hostilities.

c. *Definition.* "Material support or resources" means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (one or more individuals who may be or include oneself), and transportation, except medicine or religious materials.

d. *Maximum punishment.* Confinement for life.

(26) WRONGFULLY AIDING THE ENEMY.

a. *Text.* "Any person subject to this chapter who, in breach of an allegiance or duty to the United States, knowingly and intentionally aids an enemy of the United States, or one of the co-

belligerents of the enemy, shall be punished as a military commission under this chapter may direct."

b. Elements.

- (1) The accused aided the enemy;
- (2) The accused intended to aid the enemy;
- (3) At the time of the accused's actions, the accused had an allegiance or duty to the United States; and
- (4) The accused's acts and intentions, taken together, comprised a breach of the accused's allegiance or duty to the United States; and
- (5) The conduct took place in the context of and was associated with hostilities.

c. Comment.

- (1) The means the accused can use to aid the enemy include but are not limited to: providing arms, ammunition, supplies, money, other items or services to the enemy; harboring or protecting the enemy; or giving intelligence or other information to the enemy.
- (2) The requirement that conduct be wrongful for the crime necessitates that the accused act without proper authority. For example, furnishing unprivileged enemy belligerents detained during hostilities with subsistence quarters in accordance with applicable orders or policy is not aiding the enemy.
- (3) The requirement that conduct be wrongful for this crime necessitates that the accused owe allegiance or some duty to the United States of America. For example, citizenship, resident alien status, or a contractual relationship in or with the United States is sufficient to satisfy this requirement so long as the relationship existed at a time relevant to the offense alleged.

d. Maximum punishment. Confinement for life.

(27) SPYING.

a. Text. "Any person subject to this chapter who, in violation of the law of war and with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign power, collects or attempts to collect information by clandestine means or while acting under false pretenses, for the purpose of conveying such information to an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished by death or such other punishment as a military commission under this chapter may direct."

b. Elements.

ATTACHMENT B

TITLE XVIII—MILITARY COMMISSIONS

- Sec. 1801. Short title.
- Sec. 1802. Military commissions.
- Sec. 1803. Conforming amendments.
- Sec. 1804. Proceedings under prior statute.
- Sec. 1805. Submittal to Congress of revised rules for military commissions.
- Sec. 1806. Annual reports to Congress on trials by military commission.
- Sec. 1807. Sense of Congress on military commission system.

SEC. 1801. SHORT TITLE.

This title may be cited as the "Military Commissions Act of 2009".

SEC. 1802. MILITARY COMMISSIONS.

Chapter 47A of title 10, United States Code, is amended to read as follows:

"CHAPTER 47A—MILITARY COMMISSIONS

"SUBCHAPTER	Sec.
"I. General Provisions	948a.
"II. Composition of Military Commissions	948b.
"III. Pre-Trial Procedure	948q.
"IV. Trial Procedure	949a.
"V. Classified Information Procedures	949p-1.
"VI. Sentences	949s.
"VII. Post-Trial Procedures and Review of Military Commissions	950a.
"VIII. Punitive Matters	950p.

"SUBCHAPTER I—GENERAL PROVISIONS

- "Sec.
- "948a. Definitions.
- "948b. Military commissions generally.
- "948c. Persons subject to military commissions.
- "948d. Jurisdiction of military commissions.

"§ 948a. Definitions

"In this chapter:

"(1) ALIEN.—The term 'alien' means an individual who is not a citizen of the United States.

"(2) CLASSIFIED INFORMATION.—The term 'classified information' means the following:

"(A) Any information or material that has been determined by the United States Government pursuant to statute, Executive order, or regulation to require protection against unauthorized disclosure for reasons of national security.

"(B) Any restricted data, as that term is defined in section 11 y. of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).

intending that they are to be used in preparation for, or in carrying out, an act of terrorism (as set forth in paragraph (24) of this section), or who intentionally provides material support or resources to an international terrorist organization engaged in hostilities against the United States, knowing that such organization has engaged or engages in terrorism (as so set forth), shall be punished as a military commission under this chapter may direct.

“(B) MATERIAL SUPPORT OR RESOURCES DEFINED.—In this paragraph, the term ‘material support or resources’ has the meaning given that term in section 2339A(b) of title 18.

“(26) WRONGFULLY AIDING THE ENEMY.—Any person subject to this chapter who, in breach of an allegiance or duty to the United States, knowingly and intentionally aids an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished as a military commission under this chapter may direct.

“(27) SPYING.—Any person subject to this chapter who, in violation of the law of war and with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign power, collects or attempts to collect information by clandestine means or while acting under false pretenses, for the purpose of conveying such information to an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished by death or such other punishment as a military commission under this chapter may direct.

“(28) ATTEMPTS.—

“(A) IN GENERAL.—Any person subject to this chapter who attempts to commit any offense punishable by this chapter shall be punished as a military commission under this chapter may direct.

“(B) SCOPE OF OFFENSE.—An act, done with specific intent to commit an offense under this chapter, amounting to more than mere preparation and tending, even though failing, to effect its commission, is an attempt to commit that offense.

“(C) EFFECT OF CONSUMMATION.—Any person subject to this chapter may be convicted of an attempt to commit an offense although it appears on the trial that the offense was consummated.

“(29) CONSPIRACY.—Any person subject to this chapter who conspires to commit one or more substantive offenses triable by military commission under this subchapter, and who knowingly does any overt act to effect the object of the conspiracy, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

“(30) SOLICITATION.—Any person subject to this chapter who solicits or advises another or others to commit one or more substantive offenses triable by military commission under this chapter shall, if the offense solicited or advised is attempted or committed, be punished with the punishment provided for the commission of the offense, but, if the offense solicited or

information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1)[.]

Charge Sheet, Specification 13. Specification 14 of the same charge alleges that PFC Manning

did, at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 18 February 2010, having knowingly exceeded authorized access on a Secret Internet Protocol Router Network Computer, and by means of such conduct having obtained . . . a classified Department of State cable titled "Reykjavik-13", willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1)[.]

Id., Specification 14.

5. On 10 May 2012, the Defense filed a motion to dismiss Specifications 13 and 14 of Charge II for failure to state an offense. In that motion, as well as in its Reply Motion, the Defense urged this Court to adopt the narrow interpretation of the phrase "exceeds authorized access" – that an accused exceeds authorized access only when he bypasses technical restrictions on access and thereby obtains or alters information he is not authorized to obtain or alter – and to reject the Government's expansive interpretation of that phrase. The Defense argued that because PFC Manning was authorized to access every piece of information that he allegedly accessed, he did not exceed his authorize access under Section 1030(a)(1).

6. The Government finally provided its "definitive" theory for the phrase "exceeds authorized access" in its Response to the Defense Motion. Appellate Exhibit XCI, at 3 & n.1. In a brief moment of uncharacteristic clarity, the Government stated without qualification that "[t]he Government's theory is that the accused 'exceeded authorized access' when he violated the Government's explicit purpose-based access restriction on his SIPRNET computer." *Id.* at 3. Lest there be any lingering confusion on this point, the Government further clarified its position:

To the extent the United States did not clearly articulate its theory during oral argument on 23 February 2012, this brief, along with the theory presented during the Article 32 Investigation, should be considered the *definitive source* clarifying the Government's theory for "exceeding authorized access" on a SIPRNET computer.

Id. at 3 n.1 (emphasis supplied). In addition to belatedly providing its "definitive" theory on "exceeds authorized access," the Government also stipulated to all of the facts contained in the Defense Motion. *Id.* at 2. At no point in its response did the Government contest that PFC Manning was authorized to access each and every piece of information he allegedly accessed.

7. On 8 June 2012, this Court adopted the narrow definition of "exceeds authorized access" advocated by the Defense. See Appellate Exhibit CXXXIX, at 9. Specifically, this Court held that "the term 'exceeds authorized access' is limited to violations of restrictions on access to

information, and not restrictions on its 'use'." *Id.* (emphasis in original). At oral argument, this Court explained the proper understanding of "exceeds authorized access" as follows: "the narrow definition would be 'exceeds authorized access' would apply to 'inside hackers', individuals whose initial access to a computer is authorized but who access unauthorized information or files." See 8 June 2012 Article 39(a) audio; see also Appellate Exhibit CXXXIX, at 7.

8. The Government's "definitive" theory on "exceeds authorized access" did not stay definitive for long. Though entirely absent from the Government's Response (which the Government referred to as the "definitive source clarifying the Government's theory for 'exceeding authorized access,'" Appellate Exhibit XCI, at 3 n.1), a new Government theory made its debut during the oral argument and later in the 802 session. The Government indicated that it would attempt to show that PFC Manning exceeded his authorized access by using a particular unauthorized computer program – Wget – to download information that he was authorized to access onto his computer.¹ See 8 June 2012 Article 39(a) audio (CPT Morrow: "There are other considerations in this case, namely, as the evidence will show, the use of an unauthorized program to download information.").

9. Wget is a computer program that retrieves content from web servers, and is part of the GNU Project (a free software, mass collaboration project, announced on September 27, 1983, by Richard Stallman at MIT). Its name is derived from *World Wide Web* and *get*.² Although the program was not apparently officially authorized for the individual user, it was authorized for use on the Army Server components of the system. See Attachment A. As such, Wget is a program that is authorized to be used on certain military computers. *Id.*

10. Even while hinting at this new theory at the eleventh hour, the Government still did not dispute that PFC Manning was authorized to access all of the information he allegedly accessed.

WITNESSES/EVIDENCE

11. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the previous submissions of the parties. The Defense also requests the Court to consider the following attachments to this motion:

- a) Attachment A – email referencing authorization of Wget; and
- b) Attachment B – Classified Attachment, Intelink Logs Forensic Report, Bates # 00124331.³

¹ Consistent with its practice throughout this case, the Government has provided the Defense with the most skeletal version of its theory. Accordingly, the new Government theory articulated above is the Defense's best guess based on the cryptic description provided by the Government. As was the case with the Government's previous "definitive" theory, everyone will have to wait until the Government's Response to this motion reveals the Government's new "definitive theory" *du jour*.

² See <http://en.wikipedia.org/wiki/Wget>; see also <http://www.gnu.org/software/wget/>.

³ The Defense requests that the Government provide a copy of the specific Bates number page for the Court through the Court Security Officer.

LEGAL AUTHORITY AND ARGUMENT

12. The Government's new theory is born of convenience, not of principle. As such, it does not withstand careful scrutiny. PFC Manning's use of an unauthorized program, Wget, to download the information specified in Specification 13 of Charge II does not change and cannot change the only fact that matters in the "exceeds authorized access" inquiry: PFC Manning was authorized to access each and every piece of information he allegedly accessed. The Government is simply wrong in its theory that the use of an unauthorized program to download the information converts what would otherwise be authorized access to that information into "unauthorized access" or "exceeding authorized access." Whether or not PFC Manning used Wget to download the information is of no moment; under the language of Section 1030, as well as this Court's ruling and the great weight of authority, PFC Manning could not have exceeded his authorized access because he was authorized to obtain the information he obtained.

13. Moreover, the Government's "new" argument is simply a variation of its old "definitive" theory. Realizing that the explicit purpose-based restriction was getting it nowhere, the Government fell back on its reliance on the manner in which the information is downloaded – here, through the use of an unauthorized program, Wget – as being determinative of "exceeds authorized access." Both the Government's old theory and its new theory depend heavily on the word "so" in Section 1030(e)(6). That dependency is, for the reasons discussed by the Defense in its initial motion and reply, entirely misplaced. "Exceeds authorized access" is not concerned with the *manner* in which information is downloaded; it is rather concerned with whether the defendant was *authorized to obtain or alter the information* that was obtained or altered. Therefore, the Government's expansive interpretation, in both its old and new formulations, should be definitively laid to rest by this Court.

14. Additionally, the Government's Wget theory does not even cover Specification 14 of Charge II. The forensic evidence relied on by the Government demonstrates that PFC Manning downloaded the information referenced in that Specification directly onto his computer without using Wget.⁴ Accordingly, the Government cannot in good faith maintain that its Wget theory covers Specification 14. Therefore, as the Government has not indicated any theory other than its now-rejected explicit purpose-based restriction theory for the information in Specification 14 of Charge II, that specification should be dismissed.

15. Finally, this Court has the power to dismiss a specification where the dispositive issue is capable of resolution without trial on the general issue of guilt. The Government does not dispute that PFC Manning was authorized to access the information that he allegedly accessed. Rather, it has simply offered legal theories as to why his otherwise authorized access exceeded authorized access. The resolution of this legal issue (i.e. whether the Government states a cognizable legal theory of "exceeds authorized access") need not await trial on the general issue of guilt. Such a legal issue is instead the quintessential example of an issue capable of resolution without trial on the issue of guilt.

⁴ The very purpose of a program like Wget is to download multiple documents in a timely manner. A person would not use Wget to download one document, which can simply be downloaded by clicking "Save As" (or some variation thereof).

16. For these reasons, this Court should dismiss Specifications 13 and 14 of Charge II.

A. A Person Exceeds Authorized Access Only When He Obtains or Alters Information that He is Not Authorized to Obtain or Alter

17. A person “exceeds authorized access” under Section 1030(e)(6) only when he obtains or alters information that he is not authorized to obtain or alter. The language of Section 1030(e)(6), as well as this Court’s ruling and the great weight of authority, make this fact abundantly clear. Where, as here, it is determined that the person was authorized to access (i.e. obtain or alter) the information at issue, the “exceeds authorized access” inquiry ends. The extraneous considerations that the Government has relied on with its new and old theories – the manner in which the information is downloaded and the purpose for which the information is accessed or used – are entirely irrelevant to the “exceeds authorized access” inquiry. As the Government does not and cannot dispute that PFC Manning was authorized to access the information specified in Specification 13 of Charge II, that specification must be dismissed for failure to state a cognizable offense.

18. Section 1030(e)(6) defines “exceeds authorized access” as follows: “the term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]” 18 U.S.C. § 1030(e)(6). This definition demonstrates that the Computer Fraud and Abuse Act (CFAA) is concerned with the relationship between the accesser and the *information*: is the accesser entitled to obtain or alter the information at issue?

19. This statutory definition is not concerned with the *purposes* for which the accesser obtains or alters the information. It is also not concerned with the *manner* in which the accesser obtains or alters the information. See *Walsh Bishop Assocs., Inc. v. O’Brien*, No. 11-2673 (DSD/AJB), 2012 WL 669069, at *3 (D. Minn. Feb. 28, 2012) (“The language of [Section] 1030(a)(2) does not support the interpretation of Walsh Bishop. Instead, Walsh Bishop’s interpretation requires the court to rewrite the statute to replace the phrase ‘to use such access to obtain or alter information that the accesser is not entitled so to obtain or alter’ with ‘to use such information in a manner that the accesser is not entitled so to use.’ But subsection (a)(2) is not based on use of information; it concerns access.”). Rather, the only relevant consideration under the statutory definition of “exceeds authorized access” is whether the accesser was entitled to obtain or alter the information at issue. In this case, it is undisputed that PFC Manning was entitled to access the information. The Government’s Wget theory – that PFC Manning exceeded authorized access by using an unauthorized program to download the information – erroneously focuses on the manner in which PFC Manning downloaded the information. But the manner in which he downloaded the information is beside the point, since at all times he remained entitled to access the information in question.

20. The Government’s Wget theory is equally inconsistent with the 1996 legislative history of Section 1030, which makes clear that the CFAA targets those who access information that they are not authorized to access. As the report of the Senate Committee on the Judiciary explains, “Section 1030(a)(1) would target those persons who *deliberately break into a computer* to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments.” S. Rep. No. 104-357, at 6 (1996) (emphasis supplied). One who accesses information he is entitled to access does not in any way “deliberately break into a computer,” *id.*,

regardless of the program used to download the information. Nothing in the 1996 legislative history, or in any of the legislative history of Section 1030, provides an iota of support for the Government's theory that the manner in which information is downloaded is determinative, or even relevant, in the "exceeds authorized access" inquiry.

21. Additionally, the Government's focus on the manner in which the information is downloaded, rather than the authority to access the information, is wholly inconsistent with this Court's formulation of "exceeds authorized access." This Court properly framed the "exceeds authorized access" inquiry at oral argument: "'exceeds authorized access' would apply to 'inside hackers', individuals whose initial access to a computer is authorized but *who access unauthorized information or files*.'" See 8 June 2012 Article 39(a) audio (emphasis supplied); see also Appellate Exhibit CXXXIX, at 7. PFC Manning's use of Wget – an unauthorized program on the computer – to download the information at issue did not thereby make his *access to the information* unauthorized.

22. A simple example demonstrates why this is so. Suppose that the only authorized web browser on government computers is Internet Explorer. Suppose further that a Soldier is authorized to access certain diplomatic cables on that computer. If the Soldier used Internet Explorer to access those cables, no one – not even the Government in this case – would characterize the Soldier's actions as "exceeding authorized access." If a Soldier downloaded the web browser Firefox to the Government computer, that browser would be an unauthorized program, since the only authorized browser on the computer is Internet Explorer. Would the Soldier's use of Firefox to obtain those same diplomatic cables make the Soldier's access to those cables unauthorized? Under the Government's Wget theory, the answer would be yes. But this cannot be the case under any sensible interpretation of "exceeds authorized access." Whether he uses Internet Explorer or Firefox, the Soldier would be accessing the same cables and in both cases he would be entitled to access those cables. While the Soldier's installation of an unauthorized program on a government computer may itself be a violation of the computer use policy (and subject the Soldier to punishment under Article 92), the mere installation and use of an unauthorized program to download information cannot change the Soldier's authorization to access the underlying information.

23. So it is here. Under the Government's Wget theory, Wget was an apparently unauthorized program for the individual user. But PFC Manning did not use Wget to "access unauthorized information or files." See 8 June 2012 Article 39(a) audio. Rather, he used Wget to download information that he was authorized to access. His authorization to access that information remained unchanged irrespective of the *manner* in which he downloaded the information. Under this Court's proper formulation of the phrase "exceeds authorized access," PFC Manning did not "access unauthorized information or files." See 8 June 2012 Article 39(a) audio. Accordingly, he did not "exceed authorized access."

24. Moreover, the great weight of authority provides no support for the Government's argument that the manner in which information is downloaded can determine whether a person "exceeds authorized access." In *United States v. Nosal*, for example, the en banc Ninth Circuit explicitly tied the concept of "exceeds authorized access" to the defendant's authorization to access the particular information at issue: "'exceeds authorized access' would apply to *inside hackers* (individuals whose initial access to a computer is authorized but who access unauthorized *information or files*)." 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (second emphasis supplied);

see also Appellate Exhibit CXXXIX, at 7 (“*Nosal III* defines ‘exceeds authorized access’ to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files.” (emphasis in original)). Nothing in the definitive discussion of the narrow interpretation of “exceeds authorized access” in *Nosal* gives any indication that the manner in which a person downloads information has any bearing whatsoever on whether the person is authorized to access that information. Along similar lines, the United States District Court for the Southern District of New York recently held that “a person who ‘exceeds authorized access’ has permission to access the computer, but not the *particular information* on the computer that is at issue.” *United States v. Aleynikov*, 737 F. Supp. 2d 173, 191-92 (S.D.N.Y. 2010) (emphasis supplied). In *Aleynikov*, as here, the Government did not contest that the defendant was authorized to access the particular information at issue. See *id.* at 191 (“The Government concedes that Aleynikov was authorized to access the source code for the Trading System that he allegedly stole[.]”). The court accordingly granted the defendant’s motion to dismiss the CFAA count of the indictment. *Id.* at 194. Likewise, in a very recent Section 1030 prosecution, the United States District Court for the Central District of California found, in light of *Nosal*, that the defendant had not exceeded his authorized access because he was authorized to access the information at issue. *United States v. Zhang*, No. CR-05-00812 RMW, 2012 WL 1932843 (N.D. Cal. May 29, 2012) (finding defendant not guilty of Section 1030(a)(4) and (c)(3)(A) violations because defendant “had ‘authorized access’ to the Marvell Extranet when he downloaded the information from the Marvell Extranet in March 2005 because he had active log-in credentials at that time.”).

25. Several civil cases similarly highlight why the Government’s Wget theory cannot be sustained under the narrow interpretation of “exceeds authorized access:” the inquiry is limited to whether the *access to the information* is authorized and is not concerned with the *manner* in which that information is downloaded. See, e.g., *Ajuba Int’l, L.L.C. v. Saharia*, No. 11-12936, 2012 WL 1672713, at *12 (E.D. Mich. May 14, 2012) (holding that “a violation [of the CFAA] for “exceeding authorized access” occurs only where initial access is permitted but the access of *certain information* is not permitted.” (emphasis supplied)); *Ryan, LLC v. Evans*, No. 8:12-cv-289-T-30TBM, 2012 WL 1532492, at *5 (M.D. Fla. March 20, 2012) (“Under a narrow reading of the provisions of [Section] 1030, a violation for exceeding authorized access occurs where initial access is permitted but the access of *certain information* is not permitted.” (quotations omitted) (emphasis supplied)); *id.* at *6 (“Given that Evans and Espinosa appear to have had unfettered access to the Ryan computers, *data, information, and emails actually accessed*, with the right to add to, delete from, and upload and download matters therefrom, it is doubtful that their conduct can be brought within the purview of either [Section] 1030(a)(2)(C) or [Section] 1030(a)(4) under the narrow reading of those sections.” (emphasis supplied)); *WEC Carolina Energy Solutions, LLC v. Miller*, No. 0:10-cv-2775-CMC, 2011 WL 379458, at *4 (D.S.C. Feb. 3, 2011) (“[L]iability under the CFAA, based on an allegation that an employee exceeded authorized access, depends on whether the employee accessed *information* he was not entitled to access. WEC has not alleged that Miller or Kelley accessed information that they were not “entitled to access.” Therefore its allegation falls outside the scope of this portion of the CFAA.” (emphasis supplied)); *Nat’l City Bank, N.A. v. Republic Mortgage Home Loans, LLC*, No. C09-1550RSL, 2010 WL 959925, at *3 (W.D. Wash. March 12, 2010) (“A CFAA violation occurs only when an employee accesses *information* that was not within the scope of his or her authorization.” (emphasis supplied)); *id.* (“It is undisputed that Westmark was authorized to access, view, and utilize the Excel spreadsheet that forms the heart of plaintiff’s CFAA claim

against him. There is no indication that Westmark accessed or obtained any information from National City's computers after he resigned his position with National City. If, as is the case here, the employee were *entitled to access the materials at issue*, nothing in the CFAA suggests that the authorization can be lost or exceeded through post-access conduct. On the other hand, if an employee's access is limited to certain documents, files, or drives, an effort on his part to delve into *computer records to which he is not entitled* could result in liability under the CFAA." (citations omitted) (emphases supplied)); *Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006) ("By applying the plain meaning of the statutory terms to the facts of this case, it is clear that the Employees accessed *with* authorization, did not exceed their authorization, and thus did not violate [Section] 1030(a)(4). The analysis is not a difficult one. Because Lockheed permitted the Employees to access the company computer, they were not without authorization. Further, *because Lockheed permitted the Employees to access the precise information at issue, the Employees did not exceed authorized access*. The Employees fit within the very group that Congress chose not to reach, *i.e.*, those with access authorization. It follows that [Section] 1030(a)(4) cannot reach them. The gist of Lockheed's complaint is aimed not so much at the Employees' improper access of the ATARS information, but rather at the Employees' actions subsequent to their accessing the information. As much as Lockheed might wish it to be so, [Section] 1030(a)(4) does not reach the actions alleged in the Complaint." (emphasis supplied)).

26. In sum, the Government does not dispute that PFC Manning was authorized to access each and every piece of information covered in Specification 13 of Charge II. It instead argues that his use of Wget to download the information specified in Specification 13 renders his otherwise authorized access to that information an excess of his authorization. Such a theory finds no support in Section 1030, its legislative history, and the rulings of this Court and so many others that have adopted the narrow interpretation of "exceeds authorized access." Under that narrow interpretation of the phrase, the only inquiry is whether the accessor is entitled to obtain or alter the information at issue; the manner in which that information is downloaded does not provide an answer to that inquiry. Therefore, since PFC Manning was authorized to access all of the information covered in Specification 13 of Additional Charge II, that specification must be dismissed.

B. The Government's "New" Theory is Simply a Variation of its Already Rejected Expansive Interpretation

27. The Government's "new" theory of "exceeds authorized access" is not really a new one at all; rather, it is a slight tweak of its already rejected expansive interpretation. The explicit purpose-based restriction theory is one formulation of the expansive interpretation of "exceeds authorized access." The Wget theory, focusing as it does on the manner in which information is downloaded, is simply another formulation of this same expansive interpretation. This Court's adoption of the narrow interpretation of "exceeds authorized access" necessarily rejects both formulations of the expansive interpretation. Accordingly, this Court should dismiss the Section 1030(a)(1) specifications.

28. In an attempt to support its explicit purpose-based theory of "exceeding authorized access," the Government Response placed heavy emphasis on the word "so" in Section 1030(e)(6):

"So" means "[i]n the state or manner indicated or expressed." *Webster's II New Riverside University Dictionary* 1102 (1988). The presence of "so" after "entitled" in [Section] 1030(e)(6) makes the definition unambiguous – an individual "exceeds authorized access" when he or she obtains or alters information that he or she is not entitled to obtain or alter *in those circumstances*. Put another way, the word "so" clarifies that the user might have been entitled to obtain the information in *some other circumstances*, but not in that manner or under those circumstances. *See* 18 U.S.C. § 1030(e)(6) ("not entitled *so* to obtain or alter") (emphasis added).

Appellate Exhibit XCI, at 4 (emphases in original). The Government hoped that this expansive definition could transform otherwise authorized access to information into exceeding authorized access in some circumstances – namely, when the accessor violated explicit purpose-based restrictions on access. The Government in *Nosal* made a similar desperate attempt to hinge the expansive interpretation of "exceeds authorized access" on this expansive definition of "so:"

In its reply brief and at oral argument, the government focuses on the word "so" in the same phrase. *See* 18 U.S.C. § 1030(e)(6) ("accessor is not entitled *so* to obtain or alter" (emphasis added)). The government reads "so" to mean "*in that manner*," which it claims must refer to use restrictions.

Nosal, 676 F.3d at 857 (emphasis supplied).

29. Both this Court and the *Nosal* Court, in adopting the narrow interpretation of "exceeds authorized access," rejected this expansive definition of the word "so." The *Nosal* Court rejected this interpretation because it "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id.* This Court reiterated these concerns in its ruling. *See* Appellate Exhibit CXXXIX, at 7 ("The Court, in *Nosal III* at 857, agreed with the appellant's argument and disagreed with the prosecution's attempt to make the CFAA into 'an expansive misappropriation statute' when it was originally created as 'an anti-hacking statute.'").

30. This already-rejected "so" argument is also lingering in the background of the Government's Wget theory on "exceeding authorized access." Although the Government has yet to clearly specify its theory or the legal basis for it, there is simply no way other than the now-discredited "so" argument to get from the language of Section 1030(e)(6), which focuses on the accused's authorization to access *information*, to the Government's Wget theory, which focuses on the *manner* in which the information is downloaded. In other words, under the Wget theory, the Government argues that PFC Manning used an unauthorized program to download information that he was otherwise authorized to obtain. The Government does not dispute that PFC Manning was authorized to access this information. Thus, the only way PFC Manning's access could be unauthorized under the Government's theory is based on his access in these *circumstances*, *see* Appellate Exhibit XCI, at 4, or his access of this information in this particular *manner*, *see Nosal*, 676 F.3d at 857 – his use of Wget. Either way, the only way the language of Section 1030(e)(6) would permit such a theory would be if the word "so" had the definition advocated by the Government in *Nosal* and in this case in the Government's Response.

31. Of course, the word "so" in Section 1030(e)(6) does not have that definition. Fortunately, the Defense need not rehash the numerous arguments against the Government's definition of

"so," see Appellate Exhibit XC, at 12-13, and Appellate Exhibit XCII, at 2, 4-6, for the matter has already been definitively decided by this Court. In its ruling, this Court adopted the narrow interpretation of "exceeds authorized access" and indicated that it would give instructions "in accordance with the narrow view of *Nosal III*." Appellate Exhibit CXXXIX, at 9. This Court also clearly explained the narrow view of *Nosal*: "*Nosal III* defines 'exceeds authorized access' to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files." *Id.* at 7 (emphasis in original). By rejecting the Government's expansive interpretation and by adopting the narrow interpretation in accordance with *Nosal*, this Court properly rejected the "so" argument once and for all.

32. In the end, the Government's Wget theory is, like the explicit purpose-based theory before it, a theory on use restrictions, not a theory on access restrictions. The Government's Acceptable Use Policy (AUP) perfectly illustrates this fact. The AUP is violated when a user installs an unauthorized program, such as Wget. See Appellate Exhibit XC1, Enclosure 6, at 62 ("d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software."). Therefore, as it attempted to do with its explicit purpose-based theory of "exceeds authorized access," the Government is attempting to use a violation of a use restriction under the AUP – the installation and use of Wget – to show that PFC Manning exceeded authorized access. The problem with this effort, then and now, is that "the term 'exceeds authorized access' is limited to violations of restrictions on *access* to information, and not restrictions on its 'use'." Appellate Exhibit CXXXIX, at 9 (emphasis in original). Irrespective of any violation of a use restriction that may have occurred, PFC Manning did not hack into the computer to obtain information he was not authorized to obtain. See S. Rep. No. 104-357, at 6 (1996) ("Section 1030(a)(1) would target those persons who *deliberately break into a computer* to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments." (emphasis supplied)); Appellate Exhibit CXXXIX, at 7 ("*Nosal III* defines 'exceeds authorized access' to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files." (emphasis in original)). Instead, PFC Manning was authorized to access every piece of information he obtained.

33. For these reasons, Specification 13 of Charge II must be dismissed.

C. The Evidence Unequivocally Demonstrates that PFC Manning Did Not Use Wget to Obtain the Information Covered by Specification 14 of Charge II

34. Even putting aside the issues with the Government's Wget theory, it only applies to the information covered by Specification 13 of Charge II. It cannot apply to the information covered by Specification 14 of Charge II. Accordingly, as the Government has not articulated any theory other than its now-rejected explicit purpose-based theory for how PFC Manning exceeded his authorized access with respect to this information, Specification 14 of Charge II should be dismissed regardless of the merits of the Government's Wget theory.

35. The forensic evidence indicates that PFC Manning did not use Wget, or any other unauthorized program, to download the information specified in Specification 14 of Charge II. See Classified Attachment, Intelink Logs Forensic Report, Bates # 00124331 (forensic report indicating that the keyword "Iceland" was searched for a total of fourteen times from both of PFC Manning's primary and secondary SIPRNET computers). Instead, the forensic evidence

shows that PFC Manning simply downloaded this information directly onto his computer. *Id.* Therefore, as PFC Manning did not use Wget to download the information in Specification 14 of Charge II, the Government's new Wget theory simply cannot apply to this specification.

36. Moreover, the Government apparently has no additional theory on how PFC Manning exceeded his authorized access in obtaining this information, other than its original explicit purpose-based theory. "[T]he Government stated in oral argument that it would present evidence in addition to the AUP." Appellate Exhibit CXXXIX, at 9. The Government has indicated, albeit cryptically, its Wget theory for the information covered by Specification 13 of Charge II. Yet it has offered no additional theory for the information covered by Specification 14 of Charge II. The reason for this glaring omission is obvious: The Government has no additional theory on "exceeds authorized access" for Specification 14. Thus, the only theory of "exceeds authorized access" put forth for Specification 14 is the now-discredited explicit purpose-based theory. The Government therefore has no acceptable theory as to how PFC Manning obtained this information in excess of his authorization, and it does not contest that he was authorized to obtain this information. Accordingly, Specification 14 of Charge II must be dismissed.

D. This Court Has the Authority to Dismiss a Specification When its Underlying Legal Theory is Incorrect

37. This Court does indeed have the power to dismiss a specification where the dispositive issue is capable of resolution without trial on the general issue of guilt. The Government does not dispute that PFC Manning was authorized to access the information that he allegedly accessed. Instead, it has simply offered legal theories as to why his access exceeded authorized access. The resolution of this legal issue (i.e. whether the Government states a cognizable legal theory of "exceeds authorized access") need not await trial on the general issue of guilt. Such a legal issue is instead the quintessential example of an issue capable of resolution without trial.

38. As this Court properly recognized, it has the power to dismiss a specification before the presentation of evidence. *See* Appellate Exhibit CXXXIX, at 9 ("Federal cases dismissing charges before evidence is presented do so under Federal Rule of Criminal Procedure 12. This Court has the power to do the same under R.C.M. 907(b)(1)."). Rule 907(a) provides the standard by which a pretrial motion to dismiss is to be judged: "A motion to dismiss is a request to terminate further proceedings as to one or more charges and specifications on *grounds capable of resolution without trial of the general issue of guilt.*" R.C.M. 907(a) (emphasis supplied); *see also* R.C.M. 905("Any defense, objection, or request which is *capable of determination without the trial of the general issue of guilt* may be raised before trial." (emphases supplied)). Therefore, where the dispositive issue with the specification is entirely legal (i.e. capable of resolution without trial on the general issue of guilt), a pretrial motion to dismiss is the appropriate vehicle by which to resolve that issue.

39. The issue presented by this motion – whether the Government's theory of "exceeds authorized access" is a permissible one – is just such an issue. The issue is purely one of law: whether a particular theory of proving an essential element of the offense is legally cognizable. The Defense concedes, for the purposes of this motion, the facts alleged by the Government. Additionally, the Government has at no point disputed that PFC Manning was authorized to access all of the information specified in Specifications 13 and 14 of Charge II. The only point of disagreement between the parties is whether the manner in which PFC Manning downloaded

the information in Specification 13 – by using Wget, a program that was not authorized by the AUP – can constitute exceeding authorized access. The Defense submits that if a person is authorized to access certain files, the use of a program like Wget to download those files cannot change the fact that the person is still authorized to access those same files. This is not a factual question which must be resolved after a trial on the general issue of guilt. Instead, this is a purely legal question which is capable of resolution without any further factual development. Therefore, this Court should dismiss Specifications 13 and 14 of Charge II because the Government's legal theory of "exceeds authorized access" is not cognizable. Trial on the general issue of guilt cannot make an uncognizable legal theory a cognizable one.

40. Not only would delaying the inevitable (i.e. the conclusion that the Government cannot show, under any cognizable theory, that PFC Manning exceeded authorized access in accessing this information) until trial serve no useful purpose, an accused would suffer substantial prejudice if the Government was permitted to simply plead the elements of an offense in a specification knowing full well that it would be unable to prove an essential element at trial. To illustrate why this is so, suppose that a Soldier is charged with several crimes – for example, burglary, larceny and sexual assault of a minor. Suppose further that the Government has properly pled the elements of all of these offenses in the specifications, including the element of the sexual assault of a minor offense that the victim is a minor. If the Government has alleged in the specification that "the victim was a minor at the time of the offense" but it knows that the victim was actually nineteen years old at the time of the offense, the Soldier would suffer severe prejudice if that specification was not dismissed pretrial for failure to state an offense. Since the sexual assault of a minor specification alleges all of the essential elements of that offense, it would survive a motion to dismiss for failure to state an offense if military courts did not have the authority to dismiss adequately pled specifications based on impermissible legal theories. The Government would therefore be permitted to fully present its evidence on the sexual assault offense, all the while knowing that the "minority of the victim" element could not be satisfied. Only after the Government has fully presented its case would the Soldier be entitled to a finding of not guilty under R.C.M. 917. At that late stage, the members would have heard all about the conduct underlying the sexual assault offense. Even though the sexual assault of a minor offense would be resolved in the Soldier's favor, the members will still retire to deliberate on the burglary and larceny offenses having heard about the Soldier's conduct on the sexual assault offense. The knowledge of that unsavory conduct may lead the members to find the Soldier guilty on the burglary and larceny offenses because of extraneous, legally irrelevant considerations, such as a desire to punish the Soldier for the conduct underlying the sexual assault offense, notwithstanding the entry of a finding of not guilty on that offense, or a belief that the Soldier has a criminal character and probably committed the other offenses as well. In either case, the motion for a finding of not guilty under R.C.M. 917 cannot protect the Soldier from this danger of prejudice. The only vehicle that would adequately protect the Soldier from this danger would be a vehicle that prevents the Government from fully presenting its case based on an impermissible legal theory as to an essential element of an offense. That vehicle is the motion to dismiss for failure to state an offense under R.C.M. 907(b)(1).

41. This danger of prejudice to the accused is not confined to the hypothetical realm. In this case, PFC Manning is charged with twenty specifications in addition to Specifications 13 and 14 of Charge II. If the Government is permitted to fully present its case on Specifications 13 and 14 when its theory of "exceeds authorized access" is legally insufficient, the Government will be

permitted to put forth evidence that PFC Manning disclosed numerous diplomatic cables. As part of its proof on these offenses, the Government will also adduce evidence that the disclosure of these cables caused, or could have caused, damage to interests of the United States. While this proof is presented, the Government, the Defense, and this Court will all know that the Government's theory of "exceeds authorized access" is legally insufficient. The only group that will not know that the Government's theory is legally insufficient will be the group deciding PFC Manning's guilt or innocence: the court-martial members. While a motion for a finding of not guilty under R.C.M. 917 can ensure that the members do not find PFC Manning guilty of Specifications 13 and 14, it cannot erase from the minds of the jurors the evidence of the disclosure of the cables and the potential damage caused by the disclosure. And it cannot prevent that evidence from influencing – consciously or subconsciously – the members' determination of PFC Manning's guilt or innocence on the remaining twenty specifications. Only a pretrial dismissal for failure to state an offense under R.C.M. 907(b)(1) can prevent the danger of such grave prejudice to PFC Manning.

42. There is an additional reason why a pretrial dismissal under R.C.M. 907(b)(1), and not a motion for a finding of not guilty under R.C.M. 917, should be used to dismiss a properly pled specification based on a legally insufficient theory as to an essential element. In this case, the parties agree that clause 1 and 2 of Article 134 is a lesser-included offense (LIO) of the alleged Section 1030(a)(1) offenses, provided, of course, that the Government's legal theory underlying the Section 1030(a)(1) offenses is cognizable. If PFC Manning is forced to wait until the time for a R.C.M. 917 motion before the legally insufficient Section 1030(a)(1) offenses are resolved in his favor, the Government would get the windfall of a LIO when the original specification was legally defective and should have been dismissed outright. In other words, the Government would be able to prove a derivative offense – the LIO – even though the charged offense does not withstand legal scrutiny. Therefore, in addition to the danger that the members will use the evidence presented on the Section 1030(a)(1) offenses for improper purposes, PFC Manning would be further prejudiced in this regard. To avoid the danger of this prejudice, the Court must exercise its power to dismiss this specification pretrial pursuant to R.C.M. 907(b)(1).

43. For these reasons, this Court does have the power to dismiss a sufficiently pled specification that is premised on a legally insufficient theory as to one essential element of the offense, and this Court should accordingly exercise that power and dismiss Specifications 13 and 14 of Charge II.

CONCLUSION

44. Notwithstanding its last minute shift in theory, the Government has still not alleged that PFC Manning "exceeded authorized access" within the proper meaning of Section 1030(a)(1). PFC Manning had access to the relevant SIPRNET computers and was authorized to access every piece of information that he allegedly accessed. The Government has not disputed this crucial fact. Accordingly, because the Government has failed to allege that PFC Manning's conduct exceeded his authorized access under Section 1030(a)(1), the specifications alleging violations of Section 1030(a)(1) must be dismissed.

45. For these reasons, the Defense requests this Court dismiss Specifications 13 and 14 of Charge II because the Government has failed to allege that PFC Manning's alleged conduct exceeded authorized access.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', is positioned above the printed name.

DAVID EDWARD COOMBS
Civilian Defense Counsel

ATTACHMENT A

From: Edwards, Antonio P CIV (US) [antonio.p.edwards.civ@mail.mil]
Sent: Monday, January 23, 2012 5:52 PM
To: King, Kenneth A CIV (US)
Subject: FW: Status? (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: FOUO

See Below for Gloor answers, I am attempting to acquire, "CYGWIN and RedHat Enterprise Linux, both of which have CONS (Attached)"

Antonio P. Edwards
SPECIAL AGENT
OPMG/CID/CCIU LNO to ARCYBER

ARCYBER
8825 Beulah Street
Fort Belvoir, VA 22060
Work: (703) 706-2438
Mobile: (703) 677-2942
antonio.p.edwards.civ@mail.mil
antonio.p.edwards@ni.army.smil.mil

Washington Metro Resident Agency
CCIU, USACIDC
27130 Telegraph Rd, VA 22134
Work: (571) 305-4464
Mobile: (703) 677-2942
antonio.p.edwards.civ@mail.mil
antonio.p.edwards@us.army.smil.mil

*** CONFIDENTIALITY NOTICE ***

The information contained in this e-mail and accompanying attachments may contain confidential information which may be law enforcement sensitive. If you are not the intended recipient of this information, any disclosure, copying, distribution, or the taking of any action regarding this information is strictly prohibited. If you received this e-mail in error, please notify me immediately by return e-mail or by calling (703) 706-2438.

-----Original Message-----

From: Gloor, Thomas B LTC USARMY (US)
Sent: Monday, January 23, 2012 5:33 PM
To: Edwards, Antonio P CIV (US)
Cc: Morton, Stephen J CIV (US)
Subject: RE: Status? (UNCLASSIFIED)

Mr. Edwards,

Below are the answers to the questions you provided, I've also cc'd my Deputy- Mr. Steve Morton.

Hope this helps:

1. Was "wget" authorized for use on the SIPR computers while MANNING was in Iraq (Oct 09 to May 10).

PM DCGS-A: "wget" was authorized for use on the Server components of the system, but not on the user system, the Basic Analyst Laptop (BAL). The BAL, not the server components is the only system MANNING was authorized to use.

2. Has "wget" ever been authorized?

PM DCGS-A: See #1. "wget" was not authorized for use on the user's system, the Basic Analyst Laptop.

3. If so, has "wget" ever had a CON?

PM DCGS-A: "wget" as an individual package does not have a CON. "wget" was deployed on the Server systems as a subcomponent of other applications (CYGWIN and RedHat Enterprise Linux, both of which have CONs (Attached))

4. Regardless of authorization, or a CON, was "wget" installed prior to, or at any time after delivery?

PM DCGS-A: "wget" has never been authorized to be installed by PM DCGS-A on the user system (Basic Analyst Laptop).

5. Please provide a POC for the determination pertaining to installation, which would have occurred after delivery?

PM POC for configuration management during the questioned time was Stephen Morton, DPdM DCGS-A Intelligence Fusion, Building 6006, Aberdeen Proving Ground, Maryland 21005, Voice: 443-861-2580, DSN: 848-2580, stephen.j.morton8.civ@mail.mil. PM DCGS-A has validated that there were no user requests or Technical Bulletins to install "wget" onto the BAL.

6. Please clarify if the attached document is in fact the CON for the SIPR Iraq systems during Oct 09 to May 10?

PM DCGS-A confirms that this the correct CON.

v/r
LTC Thomas B. Gloor
PM DCGS-A Intelligence Fusion

Building 6006
C4ISR Campus
2nd Floor, Room B3-322
Aberdeen Proving Ground, Maryland 21005

NOTE NEW CELL NUMBER:
CELL: 443-835-8548
APG Voice: 443-861-2579
DSN: 848-2579

thomas.gloor@us.army.mil
thomas.gloor@us.army.smil.mil

-----Original Message-----

From: Edwards, Antonio P CIV (US)
Sent: Monday, January 23, 2012 4:25 PM
To: Gloor, Thomas B LTC USARMY (US)
Subject: Status? (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: FOUO

LTC Gloor,

I wanted to coordinate with you to determine whether you or your personnel have revealed any new information pertaining to the questions below:

I realize that it is difficult to determine whether "wget" was authorized or installed prior to delivery; however, with reference to your research, could you please exhaust any possibility of "wget" being installed prior to or after delivery, or tested and authorized but not given a CON. If so, please provide the details of the testing and authorization, and if a CON was issued, the CON. Additionally, if you believe "wget" was installed after delivery of the system, could you provide me any information you were able to find pertaining to the subsequent installation of "wget", and with a POC who would be able to confirm the details pertaining to the installation? Finally, I read over the attached document and I believe it is the CON for the Iraq SIPR system during Oct 09 to May 10, please clarify if I am incorrect?

In summary, I believe the following question remain:

1. Was "wget" authorized for use on the SIPR computers while MANNING was in Iraq (Oct 09 to May 10).
2. Has "wget" ever been authorized?
3. If so, has "wget" ever had a CON?
4. Regardless of authorization, or a CON, was "wget" installed prior to, or at any time after delivery?
5. Please provide a POC for the determination pertaining to installation, which would have occurred after delivery?
6. Please clarify if the attached document is in fact the CON for the SIPR Iraq systems during Oct 09 to May 10?

Thank you.

Antonio P. Edwards

SPECIAL AGENT
OPPMG/CID/CCIU LNO to ARCYBER

ARCYBER
8825 Beulah Street
Fort Belvoir, VA 22060
Work: (703) 706-2438
Mobile: (703) 677-2942
antonio.p.edwards.civ@mail.mil
antonio.p.edwards@ni.army.smil.mil

Washington Metro Resident Agency
CCIU, USACIDC
27130 Telegraph Rd, VA 22134
Work: (571) 305-4464
Mobile: (703) 677-2942
antonio.p.edwards.civ@mail.mil
antonio.p.edwards@us.army.smil.mil

*** CONFIDENTIALITY NOTICE ***



The information contained in this e-mail and accompanying attachments may contain confidential information which may be law enforcement sensitive. If you are not the intended recipient of this information, any disclosure, copying, distribution, or the taking of any action regarding this information is strictly prohibited. If you received this e-mail in error, please notify me immediately by return e-mail or by calling (703) 706-2438.

Classification: UNCLASSIFIED
Caveats: FOUO

Classification: UNCLASSIFIED
Caveats: FOUO

ATTACHMENT B

Forensic Report for PFC MANNING's Personal Computer

```

/Volumes/100315_0621/B98178E2-FDDC-102D-60B34786952A5C90/12 JUL 07 CZ ENGAGEMENT ZONE 30 GC
Anyone.avi
/Volumes/100215_0621/B98178E2-FDDC-102D-60B34786952A5C90/B98178E2-FDDC-102D-
60B34786952A5C90.zip
/Volumes/100215_0621/B98178E2-FDDC-102D-60B34786952A5C90/12_0950D_JUL_07_SAF_ATT_K_ON_1-
8_CAV_IN_NEW_RAGHDA0.ppt
/Volumes/100215_0621/11/w1/c3.txt
/Volumes/100215_0621/11/w1/1118_5_391_0014_08_Classified_Documents_on_Wikileaks.pdf
/Volumes/100215_0621/11/09REYKJAVIK228.txt
/Volumes/100215_0621/11/09REYKJAVIK13.txt
/Volumes/100215_0621/11/09REYKJAVIK3.txt
/Volumes/100215_0621/11/09REYKJAVIK4.txt
/Volumes/100215_0621/11/09REYKJAVIK9.txt
/Volumes/100215_0621/11/persons/Jonsson.pdf
/Volumes/100215_0621/11/persons/Skurdardottir.pdf
/Volumes/100215_0621/11/persons/Skarphedinnsson.pdf
/Volumes/100221_0411/7b31f6a.zip
/Volumes/100224_0301/
/Volumes/100302_0316/d5463a29.zip
/Volumes/100304_2258/photos/SOC10153.JPG
/Volumes/100304_2258/2010022759033858B464208699
/Volumes/100304_2258/20100304-propaganda_trans.ation
/Volumes/100304_2258/20100227_0930_arrest.pptx
/Volumes/100304_2258/20100304-propaganda_notes.
/Volumes/100304_2258/photos/SOC10151.JPG
/Volumes/100304_2258/photos/SOC10152.JPG
/Volumes/100304_2258/photos/SOC10150.JPG
/Volumes/100304_2258/photos/SOC10153.JPG
/Volumes/100304_2258/photos/SOC10154.JPG
/Volumes/100304_2258/photos/SOC10149.JPG
/Volumes/100304_2258/photos/SOC10156.JPG
/Volumes/100304_2258/photos/SOC10155.JPG
/Volumes/100304_2258/photos/SOC10148.JPG
/Volumes/100308_0142/74b39ef6.zip
/Volumes/100308_0925/
/Volumes/100311_0956/success.zip
/Volumes/100322_1255/blah.zip
/Volumes/100324_1156/6e34689e.zip
/Volumes/100329_1773/05000.zip
/Volumes/100330_1737/
/Volumes/100330_1852/
/Volumes/100331_1015/
/Volumes/100331_1542/export.csv
/Volumes/100331_1542/sp.it.zip
/Volumes/100401_1154/
/Volumes/100401_1948/105000.zip
/Volumes/100405_1225/dirflie.zip
/Volumes/100407_1255/sp.it_2.zip
/Volumes/100407_1255/sp.it.zip
/Volumes/100408_1333/
/Volumes/100410_1330/
/Volumes/100411_0918/forah.zip
/Volumes/100411_0918/sp.it.zip
/Volumes/100412_1907/overal.zip
/Volumes/100412_1726
/Volumes/100419_1656/20100419-receipt_request.pdf
/Volumes/100423_1951/12 JUL 07 CZ ENGAGEMENT ZONE 30 GC.avi
/Volumes/100427_2030/12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.vmv
/Volumes/100427_2030/cia_blah.txt
/Volumes/100504_1945/files.zip

```

(J) Figure 53 - List of identified volumes

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, [REDACTED])

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

**DEFENSE REQUEST FOR
CLARIFICATION OF
COURT RULING ON
MOTION TO COMPEL
DISCOVERY #2**

DATED: 23 June 2012

RELIEF SOUGHT

1. The Defense respectfully requests clarification/elaboration on para. 7 of p. 5 of the Court's Ruling: Defense Motion to Compel Discovery #2. The paragraph reads:

For files pertaining to PFC Manning within the possession, custody, or control of military authorities that the Government is aware of and has searched for *Brady* material, Trial Counsel must turn over to the Defense any information that is obviously material to the preparation of the defense. ...

FACTS

2. At oral argument, the Court and MAJ Fein had the following colloquy:

Court: So when you're doing reviews then, are you looking at these reviews for both 701(a)(6) and 701(a)(2)?

MAJ Fein: [pause] Ma'am for DIA information, we have been reviewing it for 701(a)(2) as well in anticipation if the Court does rule in favor based off a specific request from the Defense so we do not have to review the documents again.

Court: Okay, let's go a little bit more broadly here. When you are reviewing documents for 701(a)(2), if the Government is alerted that this could be material to the defense, the Government's got an obligation to turn this over.

MAJ Fein: The Government's ... the Government at least argues that it's not just that the documents themselves are material, it would be certain information – just like the defense is arguing or proffered to the court in their response to the *ex parte* motions of 505(g)(2). Here are the categories of information. The prosecution makes the initial determination of material to the preparation of the defense and the defense argues – provides – as they've done and then it's like "Okay, that's what we're on notice of." We're absolutely on notice that any type

of damage that resulted, for instance, is material to the preparation of the defense based off of the year and a half of requests. So as each discovery request comes in, we process it, we add it to our database of what we're reviewing and we start again, churning the review of these documents. We maintain still based off today's litigation that those documents are still not 701(a)(2), subject to the Court's order, but because we do not have a specific request. It's all documents at DIA with some caveats. Not any type, not anything directed at a certain type of information. I mean the Defense is in the best position to know exactly what was and was not compromised from their client. They could be making specific requests for what type of information they're looking for. So it's not that the Defense is an odd position of not being aware of what could be out there and if, as the Defense just stated on the record, as if the Information Review Task Force, which it was, started to review all the possible compromised documents then they should know what was compromised. We would know from reviewing the files what's there and they can make specific requests. But it goes back to, it's a generic request that's copied and pasted from 701(a)(2) for pretty much every type of document out there.

Court: What volume of information are we talking about?

MAJ Fein: Your honor, we have probably keep going, about ... I'll get you that information before we close the Court today.

...

MAJ Fein: If the Court's willing to accept the Defense's argument, that means that any document that is in the possession, custody or control of military authorities that they simply request and make no other showing, then they are entitled to inspect. Your honor, especially dealing with classified information, it goes back to ... that this is a tactic in order to essentially slow this prosecution down, slow this court martial down, on one hand arguing that, for instance, in the upcoming *Brady* motion we've given too much information for them to identify stuff and now they want everything, just because they've made a request. We've maintained, the prosecution has maintained, from the very first request, "Provide us with the specific...provide us with an adequate basis and a specific factual basis and we'll be able to process it." All documents from DIA and IRTF is not sufficient. Yes, we have prepared because we do want to move this case and we do not want to have unneeded delay in order to do this. And I have to review thousands of pages of documents again, but again, these are classified documents and the Defense notes that. And yet they still maintain a general request just because they make the request that it must be material to the preparation of the defense with no other showing.

Court: I understand that, MAJ Fein, but when the Government is reviewing these documents, the Government has a burden, an obligation, under R.C.M. 701(a)(2) to disclose material to the preparation of the defense. So if the Government while observing, while looking through these documents, sees something that you think is material to the preparation of the defense, and you're not turning it over

because they didn't ask for it, I'm going to order everything turned over to me for *in camera* review.

MAJ Fein: Yes, ma'am.

Court: So is the Government going to look at this with an eye of the defense counsel and ...

MAJ Fein: We absolutely will, ma'am. Ah - to turn over material based off of just what the Defense gives us and what they consider material to the preparation of the defense, we will review the documents for that. Cause then, that would qualify as a specific request and we would do it.

Court: We're having a circular argument here again. If you're looking at document and you say, as MAJ Fein, "Boy, if I were a defense counsel, I would find this material to the preparation of the defense" are you going to hold onto it until they request it?

MAJ Fein: No, your honor, we're not.

Court: Okay.

Mr. Coombs: ... If I didn't understand him correctly, he's free to correct me. But, I believe he said, "We have documentation that we've identified that's material to the preparation of the defense and we're prepared, if the court orders us to hand it over, to hand it over. But until we receive a specific request, we're not doing so." And if now, based upon the Court's exchange with MAJ Fein, he now realizes, "Okay, we now need to turn this over" then that's a clarification that the Defense would want to nail down. Does he have documents right now that are material to the preparation of the defense that he's been holding onto because he believed that we needed to make a specific request for it?

Court: I'll ask you that question then.

MAJ Fein: Yes, your honor. I'd ask that we can get back to the Court because we'd have literally have to look at the computer system and we'll be able to answer the Court.

Audio from Article 39(a) session, 6 June 2012. The Government never did "get back to the Court" on two issues the Court asked about:

- a) "What volume of information are we talking about?" and;
- b) "Does [the Government] have documents right now that are material to the preparation of the defense that [the Government] been holding onto because [it] believed that [the Defense] needed to make a specific request...?"

Id. In addition, the Government did not state whether it has a similar database where it kept track of documents that are material to the preparation of the defense under R.C.M. 701(a)(2) with respect to documents from HQDA; Army Criminal Investigation Command (CID); Defense

Information Systems Agency (DISA); United States Central Command (CENTCOM) and United States Southern Command (SOUTHCOM) and U.S. Cyber Command (CYBERCOM).

ARGUMENT

3. The dialogue between the Court and MAJ Fein at the previous motions argument reveals that the Government is resisting producing information that is material to the preparation of the defense at all costs. The Defense finds particularly troublesome the following exchange:

Court: I understand that MAJ Fein but when the Government is reviewing these documents, the Government has a burden – an obligation under R.C.M. 701(a)(2) to disclose material to the preparation of the defense. So if the Government while observing, while looking through these documents, sees something that you think is material to the preparation of the defense, and you're not turning it over because they didn't ask for it, I'm going to order everything turned over to me for *in camera* review.

MAJ Fein: Yes, ma'am.

Court: So is the Government going to look at this with an eye of the defense counsel and...

MAJ Fein: We absolutely will, ma'am. Ah - to turn over material based off of just what the defense gives us and what they consider material to the preparation of the defense, we will review the documents for that. Cause then, that would qualify as a specific request and we would do it.

Id. The Defense would ask the Court to consider what would have happened if the Court simply left the conversation at "I'm going to order everything turned over to me for *in camera* review", to which MAJ Fein responded "Yes, ma'am." At this point, the Court would have assumed (quite properly) that MAJ Fein understood the Court's direction to provide any information that is material to the preparation of the defense absent a specific request. It is only because the Court fortuitously asked the follow-up question, "So is the Government going to look at this with an eye of the defense counsel and..." that the Court learned that the Government had *no intention* of actually complying with the Court's order. Instead, the Government was simply planning on maintaining its firmly-entrenched position that it would only review documents when it received a "specific request."

4. In light of this conversation, the Defense believes that the Government will interpret the Court's order as narrowly and as disingenuously as possible. The Defense also believes, based on previous discovery arguments the Government has made, that the Government will take an untenable position on what information is "material to the preparation of the Defense." By way of illustration, the Government believed that the FBI investigative file pertaining to PFC Manning was *not* material to the preparation of the defense or relevant and necessary. The Court quizzically asked MAJ Fein something to the effect, "How could an investigative file *not* be material to the preparation of the defense?" Based on the Government's extremely narrow and incorrect reading of the discovery rules; its position on the FBI investigative file not being material the preparation of the defense; its position in the 6 June 2012 motions argument; its

failure to get back to the Court on certain key issues; its failure to timely disclose to the Court the existence of certain critical discovery in this case (namely, the ONCIX and FBI damage assessments); and its repeated tendency to define itself out of its discovery obligations, the Defense requests that the Court provide the following additional guidance with respect to the Government's R.C.M. 701(a)(2) obligations:

a) Specifically name the organizations that have files that fall under the R.C.M. 701(a)(2) standard. The Defense believes that this would include at least the following:

- Headquarters Department of the Army (HQDA)
- Army Criminal Investigation Command (CID)
- Defense Intelligence Agency (DIA)
- Defense Information Systems Agency (DISA)
- United States Central Command (CENTCOM) and United States Southern Command (SOUTHCOM)
- U.S. Cyber Command (CYBERCOM)

b) Clarify the Court's statement that the Government must "turn over to the Defense" "files pertaining to PFC Manning ... that the Government is aware of and *has searched for Brady material.*" (emphasis added). The Defense believes this sentence can be read as suggesting that the Government must *only* turn over only documents under R.C.M. 701(a)(2) that it has *already searched* that would qualify as "material to the preparation of the defense." The Defense thus believes that that the Government may state that the Court's order does not require the Government to turn over information that is material to the preparation of the defense for files that it *has not yet reviewed*. In other words, the Defense believes that the Government may read the Court's order as applying only retroactively and not prospectively.

c) Clarify that for files within the possession, custody and control of military authorities that that the Government has already reviewed (dating back to the beginning of the case), the Government must, if it has not already done so, review those files under the R.C.M. 701(a)(2) standard. In other words, the Defense does not believe that the Government has, for the past two years, been reviewing files within the possession, custody and control of military authorities under the R.C.M. 701(a)(2) standard. To the extent that it has not done so, the Defense requests that this Court order the Government to go back and re-review such documents under the R.C.M. 701(a)(2) standard. Any other order would reward the Government for its flagrant disregard for two years of the R.C.M. 701(a)(2) standard.

The Defense does not believe that the Government has kept a log or database for the past two years of every document within its possession, custody or control that it has reviewed and that would qualify as discoverable under R.C.M. 701(a)(2) in the event that the Government would have to produce these documents for discovery purposes. If the Government represents that it has kept such a log or database for the past two years, the Defense would ask that the Court order immediate production of that log or database; the Defense would even agree that such a document could be disclosed to the Court *ex parte* simply to demonstrate that the Government has, in fact, been keeping track of all discovery in its possession, custody and control under the R.C.M. 701(a)(2) standard for the past two years.

d) Clarify that the Court's order applies not only to files the Government has reviewed for *Brady* purposes, but also to *all* files that the Government has reviewed for its own purposes (e.g. its case in chief; sentencing; etc.).¹ In other words, if the Government has encountered any document that is material to the preparation of the defense during its case preparation, broadly construed, it must turn that document over.

e) Clarify what the "material to the preparation of the defense" standard under R.C.M. 701(a)(2) entails. The Defense submits that the Court should instruct the Government that the "material to the preparation of the defense" standard should be equated as anything that would be "helpful" to the Defense. "Helpful" in this sense means anything that is relevant and would be *helpful for the Defense to know* – not evidence that is helpful, as in favorable, to the Defense. That is, information that is detrimental to the Defense could be, and usually would be, *helpful for the Defense to know*. As argued previously, the case law reaffirms that "material" under R.C.M. 701(a)(2)(A) is not a difficult standard to satisfy. In *United States v. Cano*, 2004 WL 5863050 at *3 (A. Crim. Ct. App. 2004), our superior court discussed the content of the "materiality" standard under R.C.M. 701(a)(2)(A):

In reviewing AE V in camera, the military judge said that he examined the records and AE III contained "everything . . . [he] thought was even remotely potentially helpful to the defense." That would be a fair trial standard, but our examination finds a great deal more that should have been disclosed as "material to the preparation of the defense." We caution trial judges who review such bodies of evidence in camera to do so with an eye and mind-set of a defense counsel at the beginning of case preparation. That is, not solely with a view to the presentation of evidence at trial, but to actually preparing to defend a client, so that the mandate of Article 46, UCMJ, is satisfied.

See also *United States v. Roberts*, 59 M.J. 323, 326 (C.A.A.F. 2004) ("The defense had a right to this information because it was *relevant* to SA M's credibility and was therefore material to the preparation of the defense for purposes of the Government's obligation to disclose under R.C.M. 701(a)(2)(A).") (emphasis added); *United States v. Adens*, 56 M.J. 724, 733 (A. Ct. Crim. App. 2002) ("We respectfully disagree with our sister court's narrow interpretation that the term 'material to the preparation of the defense' in R.C.M. 701(a)(2)(A) and (B) is limited to exculpatory evidence under the *Brady* line of cases . . . As noted above, R.C.M. 701 is specifically intended to provide 'for broader discovery than is required in Federal practice . . . , and unquestionably is intended to implement an independent statutory right to discovery under Article 46, UCMJ.'). *United States v. Webb*, 66 M.J. 89, 92 (C.A.A.F. 2008) ("[U]pon request of the defense, the trial counsel must permit the defense to inspect any documents within the custody, or control of military authorities that are 'material to the preparation of the defense.' R.C.M. 701(a)(2)(A). Thus, an accused's right to discovery is not limited to evidence that would be known to be admissible at trial. It includes materials that would assist the defense in formulating a defense strategy.").

¹ At oral argument, the Court stated, "If you're looking at document and you say, as MAJ Fein, 'Boy, if I was a defense counsel, I would find this material to the preparation of the defense' are you going to hold onto it until they request it?" The Defense believes that the Court intended its ruling to apply to *all documents* with trial counsel's possession, custody and control that it reviewed – and not simply that limited sub-set of documents that the Government reviewed for *Brady*.

5. The Defense would propose a clarification to the following effect:

Under R.C.M. 701(a)(2), the Government has an obligation to turn over to the Defense any “books, papers, documents, photographs, tangible objects, buildings, or places, or copies of portions thereof, which are within the possession, custody, or control of military authorities, and which are material to the preparation of the defense or are intended for use by the trial counsel as evidence in the prosecution case-in-chief at trial, or were obtained from or belong to the accused.”

Accordingly, for any documents² that the Government has previously reviewed or will review in the future, for any purpose, that is in the possession, custody or control of military authorities, the Government must apply the R.C.M. 701(a)(2) standard. To clarify, if the Government has reviewed a document in its possession, custody or control either for *Brady* purposes or for any other purpose, the Government must also determine whether the document satisfies the R.C.M. 701(a)(2) standard. To the extent that the Government has not been reviewing documents within its possession, custody and control under the R.C.M. 701(a)(2) standard, it must re-review the documents using the correct standard. To the extent that the Government has been reviewing documents within its possession, custody and control under the R.C.M. 701(a)(2) standard, it must disclose those documents to the Defense forthwith. The Court also orders the Government to certify to what extent the Government has already been applying (or not applying) the R.C.M. 701(a)(2) standard in accordance with this order.

The documents that are subject to this portion of the Court’s order are those possessed by: HQDA; Army Criminal Investigation Command (CID); Defense Intelligence Agency (DIA); Defense Information Systems Agency (DISA); United States Central Command (CENTCOM) and United States Southern Command (SOUTHCOM); CYBERCOM; and any other agencies under military authority that the Government has not disclosed to the Court but whose files the Government has searched or has an obligation to search.

The Court also provides guidance to the Government on the R.C.M. 701(a)(2) standard. The word “material” in the expression “material to the preparation of the Defense” should not be read as being synonymous with “game-changing” or “extremely important.” Rather, the Government is obligated to disclose anything that is relevant and would be *helpful for the Defense counsel to know* as it prepares its case. The Court instructs the Government to heed the words of the Army Court of Criminal Appeals in *United States v. Cano*, 2004 WL 5863050 at *3 (A. Crim. Ct. App. 2004), “We caution trial judges who review such bodies of evidence in camera to do so with an eye and mind-set of a defense counsel at the beginning of case preparation. That is, not solely with a view to the presentation of evidence at trial, but to actually preparing to defend a client, so that the mandate of Article 46, UCMJ, is satisfied.” In addition, to be material to the preparation of the defense, the documents do not need to be admissible at trial.

² Documents should be read broadly to include “books, papers, documents, photographs, tangible objects, buildings, or places.” It should also be read to include any electronic material.

United States v. Webb, 66 M.J. 89, 92 (C.A.A.F. 2008) (“[U]pon request of the defense, the trial counsel must permit the defense to inspect any documents within the custody, or control of military authorities that are ‘material to the preparation of the defense.’ R.C.M. 701(a)(2)(A). Thus, an accused’s right to discovery is not limited to evidence that would be known to be admissible at trial. It includes materials that would assist the defense in formulating a defense strategy.”). Further, the documents do not need to be favorable – even unfavorable documents can be, and often are, material to the preparation of the Defense. If the Government has any doubt as to whether the documents should be disclosed, it should err on the side of caution and either disclose the documents or apply to the Court for *ex parte* review of the documents.

6. The Defense is certain that the Government will object to any clarification by the Court, claiming something to the effect that it “absolutely understands” the Court’s order and will comply with it. The Defense believes that the Court should not take the Government’s representations that it understands both the letter – and the spirit – of the Court’s order at face value. If the Government truly is planning on complying with the Court’s order, there should be nothing objectionable about additional clarification in this matter. The Defense submits that the Court should regard any objection by the Government to this clarification as evidence that the Government had not planned on complying with the Court’s order.

RELIEF SOUGHT

7. For the reasons identified herein, the Defense requests that this Court provide additional direction on para. 7, p. 5 of the Court’s Ruling: Defense Motion to Compel Discovery #2.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

Prosecution Response
to Defense Motion for Modified Relief
for Defense Reply
to Prosecution Response to
Supplement to Defense Motion to
Compel Discovery #2

20 June 2012

RELIEF SOUGHT

The prosecution respectfully requests that the Court deny the Defense Motion for Modified Relief for Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2 (Defense Motion). Rule for Court Martial (RCM) 701(a)(6) does not support the defense's request to suspend the proceedings and require the prosecution to state the steps it has taken to comply with its obligations as required by *Brady v. Maryland*, 373 U.S. 83 (1963) and RCM 701(a)(6).

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the defense bears the burden of persuasion and must prove any factual issues necessary to decide this motion by a preponderance of the evidence. *See Manual for Courts-Martial, United States*, RCM 905(c) (2012).

FACTS

1. The prosecution disputes the facts as characterized in the Defense Motion with respect to Defense's allegations of the Prosecution's failure to satisfy its discovery obligations.
2. On 25 April 2012, the Court found no discovery violation by the prosecution. Appellate Exhibit LXVIII ¶ 13.
3. Referral of this case occurred on 3 February 2012. Appellate Exhibit LXVIII ¶ 7.
4. The defense moved to compel the discovery it desires on 14 February 2012, 11 days after referral. Appellate Exhibit LXVIII ¶ 12. Thereafter, discovery has been the subject of extensive and ongoing litigation. *See* Appellate Exhibit VIII; Appellate Exhibit XVI; Appellate Exhibit XXVI; Appellate Exhibit XLVIII; Appellate Exhibit LIII; Appellate Exhibit XCIII; Appellate Exhibit XCIV; Appellate Exhibit XCV; Appellate Exhibit XCVI; Appellate Exhibit Appellate Exhibit XCVII; Appellate Exhibit XCVIII; Appellate Exhibit XCIX; Appellate Exhibit C; Appellate Exhibit CI.

APPELLATE EXHIBIT 172
PAGE REFERENCE
PAGE ____ OF ____ PAGES

WITNESSES/EVIDENCE

The prosecution does not request any witnesses be produced for this response. The prosecution respectfully requests that the Court consider the referenced Appellate Exhibits and their enclosures.

LEGAL AUTHORITY AND ARGUMENT

The Court should not suspend the proceedings and order the prosecution to state the steps it has taken to comply with its discovery obligations under *Brady* and RCM 701(a)(6) because nothing in 701(a)(6) nor case law sets forth any such precedent.¹ Even were there precedent for such a request, there is no basis for the request because the prosecution continues to comply with its discovery obligations and will continue to do so, or the prosecution has litigated in good faith and will comply with all Court orders.

I. THE PROSECUTION SHOULD NOT BE REQUIRED TO STATE THE STEPS IT HAS TAKEN TO COMPLY WITH ITS OBLIGATIONS UNDER *BRADY* AND RCM 701(A)(6)

A. The prosecution has and continues to comply with its obligations under *Brady* and RCM 701(a)(6).

RCM 701(a)(6) requires that trial counsel, “as soon as practicable, disclose to the defense the existence of evidence known to the trial counsel which reasonably tends to: (A) [n]egate the guilt of the accused of an offense charged; (B) [r]educe the degree of guilt of the accused of an offense charged; or (C) [r]educe the punishment.” RCM 701(a)(6) is the military’s *Brady* rule. *United States v. Williams*, 50 M.J. 436, 441 (C.A.A.F. 1999). Due process requires the prosecution to disclose evidence favorable to the accused, but only when the evidence is “material” to guilt or punishment, *Brady*, 373 U.S. at 87, or may be used to impeach the credibility of prosecution witnesses, *Giglio v. United States*, 405 U.S. 150, 154 (1972); see generally *United States v. Jones*, 52 M.J. 60, 66 (C.A.A.F. 1999). The prosecution must exercise due diligence in searching its own files, the files of law enforcement authorities that have participated in the investigation of the subject matter of the charged offenses, investigative files in a related case maintained by an entity “closely aligned with the prosecution,” and other files, as designated in a defense discovery request, that involve a specific type of information within a specified entity. *Id.* at 44.

However, the defense does not possess an unlimited right to discovery.² Relevant rules, statutes, case law, and due process define the prosecution’s discovery obligations. See *United*

¹ Accordingly, the defense cites no case law nor statutory authority for the proposition that the prosecution should state the steps it has taken in complying with its *Brady* obligations under RCM 701(a)(6). However, the prosecution does not dispute that the Court possesses the authority to order such an accounting; rather, the prosecution notes that such an order is without precedent in both the military and federal systems.

² This Court has also held that there are limits by deciding that neither RCM 701(a)(6) nor *Brady* requires the Government to identify or separate what material it discloses in discovery as *Brady* material. Appellate Exhibit

States v. Agurs, 427 U.S. 97, 106 (1976) (“[T]here is, of course, no duty to provide defense counsel with unlimited discovery of everything known by the prosecutor”). For instance, “[a] criminal defendant is not entitled to know everything that a Government investigation – particularly one this far-reaching – has unearthed when such information is not used against him at trial.” *United States v. Arroyo-Angulo*, 580 F.2d 1137, 1144 (2d Cir. 1978). Moreover, defense may not make the circular argument that discovery is necessary to determine whether discovery is warranted. See *United States v. Leung*, 40 F.3d 577, 583 (2d Cir. 1994) citing *Pennsylvania v. Ritchie*, 480 U.S. 39, 59-60 (1987) (“[C]riminal defendants have no constitutional right to know the contents of Government files in order to present arguments in favor of disclosure.”). Finally, although the RCM and military case law encourage open discovery, the defense does not have a right to discovery prior to referral under RCM 701 or *Brady*.³ Appellate Exhibit LXVIII ¶ 7.

Here, the prosecution has endeavored to disclose all evidence and discoverable information within the prosecution’s files. Moreover, the prosecution continues to endeavor to disclose all evidence and information within those files the prosecution must search as soon as possible after receipt of appropriate approvals for classified information, if applicable, to avoid further delay. The Defense Motion states that “[t]he Government should not be able to circumvent its discovery obligations for two years. . . .” As the prosecution has repeatedly emphasized, the process is time consuming given the nature of the misconduct. The volume and classification of the compromised information necessitates classification reviews and approvals from numerous entities. The prosecution has not circumvented any discovery obligation; rather, the prosecution continues to comply with its legal and ethical requirements relating to discovery. See Appellate Exhibit LXVIII ¶¶ 6, 8; U.S. Dep’t of Army, Pam. 27-26, Rules of Professional Conduct for Lawyers para 3.4(d) (1 May 1992). Additionally, the United States has disclosed more broadly than the rules of discovery require. For example, the prosecution disclosed FBI information regarding the accused’s travel and bank records that was not required to be produced under RCM 701(a)(6) nor *Brady*. *Brady* materials have been and will continue to be provided to the defense, which exceeds the requirement of disclosing the mere existence of the materials or making them available for inspection. See *United States v. Serfling*, 504 F.3d 672, 678 (7th Cir. 2007) (holding that advising the defense of the availability of a large set of documents satisfies *Brady*). This timely provision of materials satisfies the United States’ obligations under RCM 701(a)(6) and *Brady*. Despite the volume of information the prosecution has searched, the prosecution further notes that its search thus far has yielded little favorable and material information.⁴

XXXXI ¶ 6 citing *US. v. Warshak*, 631 F.3d 266, 296-97 (6th Cir. 2010) (declining to order the Government to organize and index discovery when not required by Federal Rule of Criminal Procedure 16).

³ Additionally, the prosecution does not have authority to compel production of evidence from other government agencies under RCM 703(f)(4)(A) or contest discovery issues before a military judge until after referral. Appellate Exhibit LXVIII ¶ 8.

⁴ The lack of exculpatory or mitigating information does not reflect upon the prosecution’s due diligence; rather, it reflects the accused’s culpability and the impact of his charged conduct.

B. The defense request is groundless where the prosecution continues to comply with its *Brady* obligations and the trial on the merits has yet to commence.

Absent misconduct, a *Brady* violation does not occur until the completion of trial.⁵ See *Agurs*, 427 U.S. at 103 (stating that *Brady* applies in three situations, each involving discovery of information *after trial* known to the prosecution but unknown to the defense) (emphasis added); *United States v. Jackson*, 59 M.J. 330, 334 (C.A.A.F. 2004) (noting that relief is given only if there *would have been* a different result at trial) (emphasis added); see also *Harris v. Kuba*, 486 F.3d 1010, 1015 (7th Cir. 2007) (stating that evidence is suppressed if the prosecution fails to disclose it before it is too late for the defendant to make use of the evidence and the evidence was not otherwise available to the accused through the exercise of reasonable diligence); see generally *Williams*, 50 M.J. at 441.

Here, the Court has found neither prosecutorial misconduct nor a discovery or *Brady* violation. Appellate Exhibit LXVIII ¶¶ 6, 8. Moreover, the Defense Motion prematurely claims that the discovery process has already prejudiced the accused because “there is no way the Defense can adequately prepare its case” given the amount of time between the completion of discovery and the beginning of trial. See Defense Motion ¶ 29. In particular, the defense has outlined that it contemplates a period of at least sixty days after discovery to prepare for trial. See Appellate Exhibit II (setting voir dire more than 60 days after proposed completion of discovery). Since defense’s drafting of the Defense Motion, the trial date has been rescheduled no earlier than November 2012 and potentially in January 2013. See Court Statement on the Record, 8 June 2012 Article 39a. Accordingly, the new trial date should assuage defense concerns about its trial preparation.

Still, the defense raises anew complaints of the timing of receiving discovery without regard to the motions it has submitted to the Court.⁶ See, e.g., Appellate Exhibit XXXI, Appellate Exhibit XLVIII, Appellate Exhibit LVII, Appellate Exhibit LXII; cf. Appellate Exhibit LXVIII (“[A]bsent the unanticipated filing of additional motions . . . [l]itigation of disputed discovery is taking place well before trial.”). Specifically, the defense repeatedly has made the unorthodox claim that federal agencies, including the Department of Justice and Department of State, among others, are military authorities under RCM 701(a)(2). See Appellate Exhibit XCVI

⁵ Misconduct, including gamesmanship, constitutes a *Brady* violation no matter the timing. The prosecution has conducted discovery in good faith and will continue to do so.

⁶ Both the defense, Defense Motion ¶ 30 (“[T]his is a complicated case involving a great deal of information”), and the prosecution, see, e.g., Appellate Exhibit XVI at 1; Appellate Exhibit XLIX at 3; Appellate Exhibit XCIV at 3, have noted the complexity of discovery in this case, especially given the large amount of classified information. Accordingly, the prosecution has envisioned discovery continuing until 3 August 2012. See Appellate Exhibit XLV. The numerous and unanticipated defense motions have affected the trial date. Compare Appellate Exhibit I (contemplating motions, *inter alia*, for speedy trial; member instructions; unlawful command influence; improper referral; dismissal of charges; jurisdictional defects; constitutional challenges to UCMJ, MREs, and RCMs; MRE 404(b) disclosures, MRE 304 disclosures) with Appellate Exhibit XLV (contemplating most of the aforementioned motions and, *inter alia*, motions in *Limine*; motions to suppress; pre-admission and authentication of evidence; motion to dismiss Article 104 offense; motion to dismiss specification of charge II; unreasonable multiplication of charges motion; renewal for bill of particulars; motion to dismiss all charged offenses under 18 U.S.C. § 793(e); motion to dismiss all charged offenses under 18 U.S.C. § 1030(a)(1); motion for proposed lesser included offenses; motion to compel discovery #2; and requests for judicial notice).

¶¶ 9-17. In response to such novel arguments, the prosecution has litigated the scope of discovery in good faith and in accordance with legal precedent. *See Agurs*, 427 U.S. at 106 (stating that a prosecutor may respond to a *Brady* request by submitting the problem to the trial judge).

Citing the prosecution's legal arguments twenty-five times, the Defense improperly equates discovery litigation with an alleged discovery violation. *See* Defense Motion ¶¶ 5-6, 8-10, 12, 15-16, 18-19, 21-23; *cf. United States v. Bumgarner*, 49 C.M.R. 770, 772 (A.C.M.R. 1974) (noting importance of objecting to maintain the adversarial system). However, despite the numerous citations to prosecution responses, the defense does not explain how a statement of the prosecution's steps in complying with its obligations under *Brady* and RCM 701(a)(6) would alleviate the allegations conjured by the defense. Indeed, the defense attempts to make prosecution responses to defense motions the basis of its motion requesting unprecedented relief without explaining how the relief will cure the hypothetical prejudice that has not occurred.⁷ Lacking legal justification, the defense motion should be denied.

II. IN THE ALTERNATIVE, THE PROSECUTION REQUESTS THAT THE STATEMENT BE FILED *EX PARTE*

Assuming, *arguendo*, the Court orders the prosecution to submit the statement of the prosecution's steps to comply with its obligations under *Brady* and RCM 701(a)(6), the prosecution respectfully requests the statement be filed *ex parte*. Any statement of steps taken in compliance with discovery obligations necessarily reveals insights into the Government's preparation for litigation, including motions practice, the trial on the merits, its intended sentencing case, and sensitive matters which the government does not intend to use for sentencing, and is therefore work product and not discoverable. Moreover, prosecution work product will contain classified information for which the Defense does not have approval to review; any disclosure would necessitate going through the approval process. Additionally, the accounting could serve as a springboard for further exploratory discovery requests and litigation. *See Leung*, 40 F.3d at 583. Accordingly, the prosecution requests the filing be made *ex parte*.

If the Court requires the prosecution to submit the statement in any form, the prosecution also respectfully requests thirty days to create the statement because the prosecution's ongoing discovery efforts cannot simply be suspended; the prosecution must continually track and organize the voluminous discovery with over sixty government agencies. The prosecution also submits that the delay should be attributable to the defense for speedy trial purposes because the defense made the request for relief without precedent.

⁷ The defense request for relief consists of two components: 1) a statement of the steps the prosecution has taken to comply with its *Brady* obligations under RCM 701(a)(6), and 2) a suspension of the proceedings to allow for the completion of the first component. The statement requested in the Defense Motion would not cure the issues it alleges. Without a justification for the statement, the need for the suspension of proceedings is moot. If the defense desires a delay, it should submit a motion rather than requesting the Court suspend the proceedings under the guise of the Defense Motion.

CONCLUSION

For the foregoing reasons, the prosecution respectfully requests that the Court deny Defense Motion for Modified Relief for Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2.



ALEXANDER S. VON ELTEN
CPT, JA
Assistant Trial Counsel



ASHDEN FEIN
MAJ, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 20 June 2012.



ASHDEN FEIN
MAJ, JA
Trial Counsel

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, [REDACTED])

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

**DEFENSE RESPONSE
TO GOVERNMENT
DUE DILIGENCE
SUBMISSION
DATED 20 JUNE 2012**

22 June 2012

RELIEF SOUGHT

1. The Defense moves for the Court to order the Government to provide a due diligence accounting of the steps it has taken to comply with its *Brady* obligations.

BURDEN OF PROOF

2. As the moving party, the Defense has the burden of persuasion. R.C.M. 905(c)(2)(A). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

WITNESSES/EVIDENCE

3. The Defense requests that this Court consider the following evidence: Attachment - SGT Bradley email on 27 February 2012.

4. The Defense has also requested the following witnesses:

a) A witness from the Office of the National Counterintelligence Executive (ONCIX) who can testify to:

- i) the representation made to trial counsel in February 2012;
- ii) the representation made to trial counsel in March 2012;
- iii) what ONCIX had by way of a damage assessment in February and March 2012; and
- iv) the contents of the 18 May meeting with ODN1.

b) A witness from the Federal Bureau of Investigation (FBI) who can testify as to when the FBI had something by way of a damage assessment/impact statement, and when trial counsel had knowledge of this fact.

c) A witness from the Department of Homeland Security (DHS) who can testify as to when the DHS had something by way of a damage assessment, and when trial counsel had knowledge of this fact.

The Court has denied this request as being untimely. The Court has also ruled that these witnesses are not relevant and necessary for the Court to rule on the Due Diligence Motion.

FACTS

5. The Defense incorporates the factual assertions from Appellate Exhibit XCVI (Defense Motion to Compel Discovery #2); Appellate Exhibit XCVIII (Defense Reply to Government Response to Motion to Compel Discovery #2); Appellate Exhibit XCIX (Supplement to Defense Motion to Compel Discovery #2); Appellate Exhibit CI (Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2; Defense Motion for Modified Relief); Appellate Exhibit CXX (Defense Response to Prosecution Notice to Court of ONCIX Damage Assessment); and the Defense's filings of 18 June 2012 and 21 June 2012 requesting witnesses for the purpose of this motion. The Defense also requests the Court to consider the filing by the Government on 20 June 2012 (Prosecution Response to Defense Motion for Modified Relief for Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2).

ARGUMENT

6. The Government latest Response reveals its new strategy – if you can't respond to the issues at hand, change the topic. The Defense has chronicled, in painstaking detail, the serious questions that exist about all the outstanding discovery (particularly *Brady* discovery) in this case. See Appellate Exhibit XCVI (Defense Motion to Compel Discovery #2); Appellate Exhibit XCVIII (Defense Reply to Government Response to Motion to Compel Discovery #2); Appellate Exhibit XCIX (Supplement to Defense Motion to Compel Discovery #2); Appellate Exhibit CI (Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2; Defense Motion for Modified Relief); Appellate Exhibit CXX (Defense Response to Prosecution Notice to Court of ONCIX Damage Assessment); Defense's filings of 18 June 2012 and 21 June 2012 requesting witnesses for the purpose of this motion

7. Among the issues raised:

- a) Why didn't the Government tell the Court about the ONCIX damage assessment?
- b) Why did the Government represent that it had searched the files of 63 agencies prior to February 2012 and found no *Brady*, but now is saying that it

- did not begin its *Brady* search until February 2012 after ONCIX informed the Government that it needed to go to these agencies?
- c) When did the Government learn of the FBI impact statement? (*not* when did the Government get approval to tell the Defense about the impact statement?). When did the FBI begin the impact statement? When did it complete the impact statement?
 - d) When did the Government learn of the Department of Homeland Security damage assessment? Why didn't the Government tell the Court about this at the 6 June 2012 motions argument, given that the parties and the Court were in the process of discussing what damage assessments existed?
 - e) Why didn't the Government ever follow-up with HQDA? Why did it take someone at HQDA, nine months after the original memo was circulated, to realize that nobody had conducted a *Brady* search?
 - f) Why hadn't the Government already searched the files of the Department of State? How can it be that two years into the case, the only document from the Department of State that the Government has seen is their damage assessment?
 - g) Why has the Government not completed a *Brady* search of documents that it agrees are under military possession, custody and control?
 - h) Why has the Government not yet completed a *Brady* search of closely aligned agencies?

8. After the Defense filed Appellate Exhibit CXX (Defense Response to Prosecution Notice to Court of ONCIX Damage Assessment) and Appellate Exhibit C1 (Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2; Defense Motion for Modified Relief), the Government stated that it needed an additional two weeks to respond to matters raised therein. On 20 June, 2012, the Government filed its response. Shockingly, the Government has not responded *to a single* issue raised by the Defense. The Government does not mention the ONCIX damage assessment, the FBI impact statement, the DHS damage assessment, the HQDA memo – or anything factual about this case. Instead, the Government essentially asks the Court to, “trust us, we know what we are doing.”

9. The whole point of allowing the Government two weeks to respond was to provide answers to the factual issues raised by the Defense, not to allow the Government to rehash its arguments that there is no basis for ordering a due diligence statement. The Government already made *those exact same arguments* on 24 May 2012. See Appellate Exhibit XCVII (Prosecution Response to Defense Motion to Compel Discovery #2) (“The prosecution respectfully requests that the Court deny the defense’s request for the prosecution to respond to inquiries related to its due diligence search for discoverable information. There is no legal authority to support the defense’s request. Should the Court be inclined to [grant the Defense’s motion], the prosecution requests leave of the Court to require the prosecution to prepare internal memoranda and other attorney work-product, and present this information to the Court *ex parte* ... based on it being attorney work-product”).

10. The purpose of deferring argument for two weeks was to enable the Government an opportunity to explain to the Court inconsistencies in the factual issues raised by Defense’s

motion. That is *the basis upon which* the Court granted a two-week extension. If the Government was going to use the two-week extension to simply regurgitate old arguments and repeat that “the prosecution continues to comply with its discovery obligations and will continue to do so” and “the prosecution has and continues to comply with its obligations under *Brady*” (See Government Response at p. 2), there was absolutely no need for this two-week extension.

11. To recap, the Government revealed for the first time a couple of weeks ago that the FBI had prepared a damage assessment/impact statement. In Appellate Exhibit CI (Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2; Defense Motion for Modified Relief), the Defense argued:

Second, the Government casually mentions that it “discovered that the FBI conducted an impact statement, *outside of the FBI law enforcement file*, for which the prosecution intends to file an *ex parte* motion under MRE 505(g)(2).” Government Response to Supplement, p. 4. What does the Government mean that it “discovered” that the FBI conducted an impact statement? The Government and the FBI engaged in a joint investigation of the accused and are closely aligned. The Defense has repeatedly asked for documents from the FBI; moreover, the Government has a duty to turn over *Brady* even in the absence of a Defense Request. See Government Response to Supplement, p. 6 (“The prosecution shall, and will, disclose Brady ... even in the absence of a defense request.”).

On 20 January 2012, the Defense made the following discovery request: “Does the Government possess any report, damage assessment, or recommendation as a result of any joint investigation with the Federal Bureau of Investigation (FBI) or any other governmental agency concerning the alleged leaks in this case? If yes, please indicate why these items have not been provided to the Defense. If no, please indicate why the Government has failed to secure these items.” See Attachment L to Appellate Exhibit VIII at paragraph 3(b). On 31 January 2012, the Government responded: “The United States will not provide the requested information. The defense has failed to provide any basis for its request. The United States will reconsider this request when provided with an authority that obligates the United States to provide the requested information.” Attachment N to Appellate Exhibit VIII, paragraph 3(b).

Apparently, despite the Defense’s discovery request, the Government did not disclose the existence of the FBI impact statement in January. When was the impact statement prepared? Why is the Government only now “discovering” its existence, as if by happenstance, three months before trial? Presumably, the impact statement is something that has been in the works for a while. In other words, the FBI impact statement did not just magically appear out of thin air. Why has the Government not disclosed its existence to the Defense or to the Court? This latest revelation by the Government shows that the Court and the Defense are left completely in the dark about relevant documents that exist in closely aligned agencies until the Government decides, at its convenience, to

confirm or reveal their existence. Further, the Government states that it intends to produce any *Brady* material “as soon as possible; however, the current case calendar outlines MRE 505 proceedings to take place a future date.” Government Response to Supplement, p. 4. The subtext of this statement is that it will be months before the Defense gets access to the FBI’s impact statement.

Id. p. 10-11.

12. At oral argument, the Court asked MAJ Fein *when* the Government learned about the FBI impact statement.

COURT: Alright, we will be addressing that aspect of this motion at the next session. I understand the Defense’s argument. Government, are you prepared to tell me when you did know about this impact statement or impact assessment?

MAJ Fein: Your Honor, the Government would like to at least have a chance to argue the due diligence argument first and then answer that in (inaudible) Court’s order.

Article 39(a) Audio Recording 6 June 2012. MAJ Fein seemed to indicate that he would provide an answer to the Court’s very straightforward question as part of the Government’s due diligence submission, for which he had requested a two-week extension. MAJ Fein did not address the FBI impact statement *at all* in the Government’s 20 June 2012 submission.

13. The Defense believes that the Government has known about this impact statement for a long time. It bases this belief on the fact that on 22 March 2012, the Government stated in its disclosure to the Court, “the United States is concurrently working with other Federal Organizations which we have a good faith basis to believe may possess damage assessments or *impact statements*....” See Prosecution’s Response to Court’s Email Questions (22 March 2012). The Defense believes that the “impact statement” the Government was referring to on 22 March 2012 was the FBI impact statement (because all other documentation which assessed harm had been previously referred to as “damage assessments”). The Defense also believes that the Government was referring to the FBI impact statement on 20 April 2012 when it represented that “the United States anticipates that the FBI is the only government entity that is a custodian of classified forensic results or investigative files relevant to this case that will seek limited disclosure IAW MRE 505(g)(2).” Appellate Exhibit LVI. The Defense believes that the limited disclosure which the Government anticipated the FBI seeking was in respect of the impact statement (not forensic results or investigative files).¹

14. Moreover, the Government has still not explained other problematic issues in this case. For instance, the Defense raised the HQDA memo (which showed that the Government forgot about

¹ It is worth noting that the Government would use the terminology of “forensic results” or “investigative files” to refer to the impact statement. This underscores how the Government chooses to argue that certain terms are “terms of art” only when it suits the Government’s purposes. The Government similarly used “damage assessment” to refer to documents that it previously had stressed must be referred to as “working papers.” See Appellate Exhibit CI, para. 14.

its *Brady* search within the Department of the Army) as an illustration of the lack of due diligence on the part of the Government. The Defense argued that if the Government cannot be trusted to conduct a *Brady* search in its own backyard, it cannot be trusted to conduct a *Brady* search of numerous federal entities. The Government has not once responded to the Defense's argument – other than to say that responses to the HQDA memo should not be discoverable. It has not provided *any* explanation as to why it did not follow-up with HQDA for none months on the *Brady* search.

15. The Government has also not provided any written account of why it did not notify the Court that ONCIX was conducting a damage assessment. All the Court has to go on is the Government oral representations at the 6 June 2012 39(a) session that the Government simply repeated what it was told by ONCIX. For reasons discussed in more detail below, the Government's account simply does not ring true.

16. Similarly, the Government has not explained why it has not yet searched *any* non-investigative records at the Department of State, even though this case has been ongoing for over two years. By its own admission, the only document from the Department of State prior to 6 June 2012 was the Department of State damage assessment, which it reviewed only a couple of days before disclosing it to the Court. The Government has not answered – much less, satisfactorily answered – why it has not reviewed any non-investigative Department of State files (or even made inquiries) in the two years since PFC Manning was incarcerated. PFC Manning is charged with releasing hundreds of thousands of Department of State cables. One would think that a diligent prosecutor would, sometime in a two-year time period, think to review documents from the Department of State for *Brady*.

17. Equally, the Government has not explained why it is still “in the process” of conducting a *Brady* search of almost every agency involved in this case. As the Court went through each and every agency involved in this case, the Government's refrain was some variation of “we are in the process of conducting a *Brady* search.” See Article 39(a) Audio Recording 6 June 2012. How can it be that two years into the case the Government is still “in the process” of conducting a *Brady* search?

18. In short, the Government has not answered any factual questions about its *Brady* search that would allay any of the Defense's or Court's concerns about the diligence of the Government. If anything, the more the Government says, the more the Defense is concerned that the Government is dropping the ball with respect to its *Brady* obligations. Fundamentally, there is one overarching fact that simply cannot be ignored: more than 24 months since PFC Manning was arrested, the Government has still not even begun searching some critical files. This fact alone – without knowing anything else – should give a Court great pause about the Government's diligence.

19. The Government maintains that it should not have to provide any factual detail, unless ordered to do so by the Court. In opposing the Defense's request for witnesses, the Government states:

The United States objects to the Court's reconsideration of its ruling that the witnesses are not relevant and necessary and that the defense's request was untimely. On 2 June 2012, the defense motioned the Court to require the government to provide a diligence statement and, at the motions hearing on 6 June 2012, the government requested time to respond to whether the government should be required to provide a due diligence statement to the Court. Furthermore, after being asked by the Court to provide specific dates on when the government received certain information, the government requested to defer answering the Court's questions about timing, until the due diligence statement motion was completely litigated.²

On 20 June 2012, the government filed its response to the due diligence motion arguing that the Court should not order the government to provide a response, thus potentially making this issue moot, or in the alternative the government file a response *ex parte*. The government recognizes, that if after consideration of both parties argument (for which the defense has already argued), the Court orders the government to produce a statement, then the government will comply with the Court's order.

Prosecution Response to Defense Motion to Request Reconsideration of Addendum #2 to Defense Motion to Compel Discovery #2: Request for Witnesses, p. 2. At bottom, what the Government is saying is that it simply will not answer any questions unless the Court orders it to.³ The dates on which MAJ Fein made certain inquiries is not a national secret; it should not require an order from a military judge for MAJ Fein to disclose to the Court when he learned of the existence of, for instance, the FBI impact statement.

20. In light of the refusal of the Government to answer any factual questions in this case absent a Court order, the Court should take the Defense's factual statements as uncontroverted and order the relief sought by the Defense.

I. The Government's Account of Events Surrounding the ONCIX Damage Assessment Does Not Make Sense

21. The Government's version of events concerning the ONCIX damage assessment brings to mind the famous line: "Oh what a tangled web we weave, when first we practise to deceive!"⁴ The Government here indeed has woven a tangled web, and it is only by parsing carefully through that web that the Government's story completely falls apart.

² The Government is incorrect with respect to the dates of requested relief. The Defense requested a due diligence statement as part of its 10 May 2012 Motion to Compel Discovery #2 (*see, e.g.,* para. 1.c)). Consequently, the Government has had 40 days to respond to this aspect of the Motion to Compel Discovery #2. In that time, the Government has not provided any factual justification for any issues raised by the Defense (with the exception of ONCIX, addressed herein).

³ The Government's position is, unsurprisingly, nonsensical. Answering the questions that the Defense and the Court raised would assist the Court in determining whether the requested relief is appropriate.

⁴ Sir Walter Scott, *Marmion, Canto v. Stanza 17*. Scottish author and novelist (1771 – 1832); available at: http://en.wikipedia.org/wiki/Walter_Scott.

a) The Government's Phraseology Was Deliberately Designed to Mislead the Court

22. In the 15 March 2012 motions argument, the Government represented that the DOS had not "completed" a damage assessment and that ONCIX had not "completed" a damage assessment. In other words, the Government's representation with respect to DOS and ONCIX was identical. The Defense challenged this, at least with respect to DOS, noting that it was clear that the DOS was working on *something*, even though it was not completed. The Government refused to answer the Court's questions on the DOS damage assessment, saying that it was only authorized to state that the DOS had not completed a damage assessment.

23. After the motions argument, on 21 March 2012, the Court asked the Government to respond to questions regarding whether certain agencies had damage assessments. The Government's responses with respect to DOS and ONCIX were as follows:

- a) DOS – "DOS has not completed a damage assessment."
- b) ONCIX – "ONCIX has not produced any interim or final damage assessment in this matter."

See Prosecution's Response to Court's Email Questions dated 21 March 2012. In other words, the response with respect to ONCIX changed from its previous statement in the oral argument.

24. The Court and the Defense knew, based on previous oral argument and public statements, that the Government's statement regarding DOS meant that the DOS had something (i.e. a draft) – even though there was not a "completed" damage assessment. With respect to ONCIX, the Government's phraseology that ONCIX had neither a completed nor interim damage assessment was designed to deceive the Court and the Defense into believing that *nothing* existed in the hands of ONCIX.

25. If it is true that ONCIX did not have a draft damage assessment, there were many ways to phrase this. For instance, the Government could have said, "ONCIX has an ongoing damage assessment; however, they have represented to us that they do not have an interim or a final report at this time." The Government's representation to the Court on 21 March 2012 made it seem to a reasonable person that: a) ONCIX did not have a damage assessment, period; and b) the Government personally verified that ONCIX did not have anything. Neither one of these was true.

26. Moreover, the Government had numerous occasions to correct the misimpression it had created. In particular, after the Defense began receiving *Brady* materials from various agencies that were addressed to ONCIX, the Defense knew something was amiss. It broached this issue with the Government and the Court. See Attachment to Appellate Exhibit CXX. The Government, rather than coming clean and admitting that ONCIX had a damage assessment (albeit in some sort of draft form), continued its practice of obscuring the truth. This was when the Government conveniently and out of whole cloth fabricated definitions of "damage assessments" and "investigations." See Appellate Exhibit LXXII. It continued to maintain that ONCIX did not have a damage assessment (even though the Court had already concluded that

the Department of State draft/interim assessment was discoverable). And it maintained that the data collected by ONCIX, and presumably accumulated into some report, did not fall within the purview of the word "investigations." See Prosecution Brief Discussing Investigations and Damage Assessments.

b) The Government's Timeline For Its Initial Inquiries of ONCIX Does Not Make Sense

27. When one superimposes the Government's version of events upon the aforementioned, its story becomes even more suspicious. At the 6 June 2012 motions argument, the Court asked MAJ Fein a very straightforward question, which garnered a very evasive answer:

COURT: Why did you tell me back on the 21st of March that NCIX or ONCIX had no damage assessment? Those were not the exact words you used but go ahead and tell me-

MAJ Fein: Correct your Honor. Your Honor, frankly. Because we do not have access. Or even knowledge, absent us asking a question and receiving it to these files because of the nature of this type of assessment. We ask the questions based off of the Defense's discovery requests.

Article 39(a) Audio Recording 6 June 2012.

28. MAJ Fein implies that he did not have any "knowledge" of the damage assessment; he later admits that he knew the whole time that ONCIX was working on a damage assessment. So, if he knew that ONCIX was working on a damage assessment, why did he not tell the Court on 21 March? It was clear what the Court was asking at the time – did ONCIX have some type of damage assessment, whether in draft or final form? The Government deliberately mislead the Court in not supplying a full answer to the Court's question.

29. MAJ Fein then proceeds to lay out a timeline:

Specifically your Honor, if it may please the Court to kind of lay out a time line. This is, this is somewhat reflected in the Defense's motion from Saturday. But, 16 February 2012 was the Defense's motion to compel discovery, their first motion. On 28 February 2012 was the first 802 conference. *After the 16 February 2012 motion to compel, we approached at some point, I don't have that date, NCIX through ODN1 and said "we are required to produce the following, here is an example of what it is. What do you have?"* And then their response of course given was the department of, ONCIX has not completed a damage assessment – to date they have not produced any interim or final damage assessment in this matter. That is what they gave us and told us.

Id. (emphases supplied).

30. There are several problems with this statement. First, MAJ Fein indicates that sometime between 16 February 2012 and 28 February 2012, he approached ONCIX and said "we are

required to produce the following, here is an example of what it is. What do you have?" At this point, though, the Government was not required to "produce" anything. In fact, the Government's position was that the damage assessments were not relevant and necessary under R.C.M. 703. So it is unclear whether this conversation ever even took place – at least in the way that MAJ Fein relates.

31. MAJ Fein continues:

MAJ Fein: And then their response of course given was the department of, ONCIX has not completed a damage assessment – to date they have not produced any interim or final damage assessment in this matter. That is what they gave us and told us.

COURT: Did they do that orally or in writing?

MAJ Fein: Orally your Honor. And so, by us writing that down, and inquiring is this all you have, is this what it is? And this is the response we received. That is ultimately what we – fast forward, at the motions hearing, on the record, both at the 802 conference after the motions hearing.

Id.

32. Apparently, the Government is saying that someone from ONCIX orally (presumably by phone) notified the Government that "ONCIX has not produced any interim or final damage assessments in this matter" and that the Government wrote it down and represented that to the Court verbatim in the February motions argument. Unfortunately for the Government, that is not what the Government said at the oral argument. Instead, it stated that ONCIX has not "completed" a damage assessment. Article 39(a) Audio Recording 15 March 2012. So even under its own version of events, the Government is not accurately relaying what ONCIX apparently told them. This is probably because these conversations did not happen – or at least did not happen in the way that the Government suggests.

33. The Government then states that, after the Court sent the email questions on 21 March 2012, it reached out to ONCIX again on this issue prior to responding on 22 March 2012:

MAJ Fein: Yes, your Honor. And the prosecution did exactly that, your Honor. Even after the email from the Court, the prosecution reached out to ODNI and NCIX to ask the question again and this was the response we received.

Id.

34. So, apparently after reaching out to ONCIX a second time, ONCIX represented again that "ONCIX has not produced any interim or final damage assessments in this matter" and this time, the Government relayed that fact to the Court.

35. Sometime in this time period, the Government was also having conversations with the DOS and ONCIX about the differences between a “draft” and “interim” report. The Court asked MAJ Fein the following question:

THE COURT: So the Government’s position if I am understanding it then, is that you saw a distinction between the Department of State – which you told me the Department of State has not completed a damage assessment; and – I guess what is the difference between what the Department of State’s position was at that time and what ONCIX’s was at that time?

Id. Again, MAJ Fein was not able to provide an answer:

MAJ Fein: Your Honor, to be honest, the Government does not necessarily know. We asked the questions and this is what we are given and what we relayed to the Court. To us, there is a difference between a draft and an interim. A draft is an ongoing document. An interim is something that is produced as a snapshot in time, to memorialize the information. *So we did have discussions with both entities on what the differences could be, but at the end of the day we asked “do you have any documentation or do you have a damage assessment, and if not, what do you have?”* And these were the responses that we were given and that we relayed to the Court. So again, we have never maintained that we didn’t know they were doing one. In fact, I think it was publicly announced, and the Defense has notified the Court in one of the very first filings that it was publicly announced that they were doing one, but the extent of what they did – the prosecution had no clue, we had to rely on what they were told, or what we were told.

Id. (emphases supplied).

36. Importantly, MAJ Fein’s statement reveals that at some point in the time period of February-March 2012, the Government actually had “discussions” with ONCIX “on what the differences could be [between a draft and an interim report].” If the Government and ONCIX are having conversations about the (self-imposed) distinctions between a “draft” and an “interim report” so as to formulate a less-than-truthful response to the Court, there is most certainly a problem. If the Government felt it necessary to discuss the differences between a draft and an interim report with ONCIX, then clearly it knew that while ONCIX might not have an interim report, it most certainly had a draft.

37. MAJ Fein also says “but at the end of the day we asked ‘do you have any documentation or do you have a damage assessment, and if not, *what do you have?*’” *Id.* (emphases supplied). Apparently, even though MAJ Fein claims to have asked this question, either: a) ONCIX did not answer it; or b) the Government failed to communicate ONCIX’s response to the Court.

c) The Government’s Timeline of Events Post-23 March 2012 Does Not Make Sense

38. The Government says that, after the Court's ruling on 11 May 2012 regarding the DOS damage assessment, the Government went back to ONCIX to get ONCIX to reassess their position:

MAJ Fein: ... So, so the Government's position isn't that we didn't know that they weren't in the process of creating a damage assessment, but we were unaware that they had any other documentation created that would even qualify as a draft. Once we received the Court's Order on 11 May, we had them relook and reassess and that is when we started this process.

...

MAJ Fein: ... the prosecution had no clue, we had to rely on what they were told, or what we were told. And then we remedied it the moment we realized that, that, we attempted to remedy it once we realized, and asked them to reassess their position based off the Court's Order of 11 May. But they had to come back to us to say "yes, what we read actually means we have something like that. Not what necessarily we told you before." Of course, everything changes as time goes on. So, once they told us, we then went through the procedures and we are here.

...

MAJ Fein: And so, going forward your Honor, after that Ruling and then after we re-litigated the Department of State, then we sent that and said listen, essentially as we have outlined in our memo to ODNI on behalf of NCIX, and then their response back. On 11 May the Court ruled even a draft damage assessment from the Department of State is discoverable in that form. We re-litigated that. Does this, does this information apply to ya-all (sic)? Based off of what you have previously told us. And at that point they said we need to have a meeting. We had the meeting within a week.

Id.

39. There are several things that do not make sense here. If ONCIX represented to the Government that it did not have an interim damage assessment, why it is necessary to "have them relook and reassess" after the Court's Order on 11 May? If the Government genuinely believed that ONCIX did not have a draft/interim damage assessment, there would be absolutely no need to go back to ONCIX to get them to "reassess their position" and ask whether "this information appl[ies] to [ONCIX]."⁵

40. Moreover, the Court's order does not change the factual issue of whether ONCIX *has* a draft/interim report – all it says is that the DOS damage assessment is discoverable. But, in his statement, MAJ Fein makes it seem like there was something special in the Court's order which would provide guidance to ONCIX in determining whether what ONCIX had would qualify as a

⁵ By way of illustration, the Government has represented that DOJ does not have a damage assessment. After the 11 May 2012 Ruling, the Government (presumably) did not go back to DOJ to make sure that they still did not have a damage assessment.

draft/interim report: "But [ONCIX] had to come back to us to say "yes, *what we read actually means we have something like that*. Not what necessarily we told you before." *Id.* (emphases supplied). The Court's ruling does not in any way help ONCIX in determining whether ONCIX has "something like [the DOS draft]" as the ruling does not describe the DOS damage assessment. All the ruling says is that the DOS damage assessment is discoverable, even in draft form. The substantive portion of the Court's ruling reads, in its entirety, "The Court has examined both the classified letter and the classified DOS Damage Assessment and finds that the DOS Damage Assessment is a draft damage assessment. The fact that it is a draft does not make the draft speculative or not discoverable under RCM 701." See Appellate Exhibit LXXXVI, p. 1. In other words, the only thing to be gleaned from the Court's ruling is that a draft damage assessment is discoverable, *not that* what ONCIX has in its possession qualifies as a draft.

41. In reality, the Defense believes that both the Government and ONCIX knew that ONCIX had a draft or interim report at the time that the Government made its misrepresentations to the Court. What the Government and/or ONCIX did was craft a very deliberate statement which would allow them plausible deniability: "ONCIX has not produced any interim or final damage assessments in this matter." If they were ever caught, they could simply say that they never represented that ONCIX did not have a draft (which, according to the Government is distinct from an "interim" damage assessment).

42. The only thing that changed on 11 May 2012 was the Government's (and perhaps ONCIX's) belief about the legal discoverability of a draft damage assessment. This, however, does not change the underlying factual issue that the Court asked about, i.e. does ONCIX have some sort of damage assessment? The Government should not be permitted to hide facts from the Court because of a belief that those facts will not be important in light of subsequent legal rulings.

d) The Government Cannot Be Permitted to Blindly Parrot Assertions from Other Agencies

43. The Government is hiding behind what ONCIX apparently told them on several occasions to disclaim any responsibility for not being forthright with the Court. Above all, the Court should not lose sight of the fact that the Government *knew* that ONCIX was working on a damage assessment and did not share this fact with the Court or Defense. At the end of the day, this is the most troubling omission.

44. MAJ Fein repeatedly casts blame on ONCIX for the misstatements, saying that the Government simply repeated what it was told:

MAJ Fein: And then their response of course given was the department of, ONCIX has not completed a damage assessment – to date they have not produced any interim or final damage assessment in this matter. That is what they gave us and told us.

...

MAJ Fein: Orally your Honor. And so, by us writing that down, and inquiring is this all you have, is this what it is? And this is the response we received. That is ultimately what we – fast forward, at the motions hearing, on the record, both at

the 802 conference after the motions hearing, and on the email inquiry on 21 March, when asked. As you will notice from the Court's motion to compel discovery dated 23 March 2012, the Court documented the email questions and those email questions were does the damage assessment essentially exist with ODN1, or excuse me with ONCIX. And we responded in an email ONCIX has not produce any interim or final damage assessments in this matter. We asked them the questions. We don't have any other access to their files. They answered it. So, at that point we relayed that to the Court, we relayed it to the Defense and the Court ruled. Then –

...

MAJ Fein: Correct your Honor. It is our belief, at that point, that they were compiling these other assessments we knew about because we started reaching out once they told us about it – to go get those. But, that they had no other documentation that would be subject to discovery – based off this response.

...

MAJ Fein: We asked questions, we give them the relevant cases, the case law, we show them the discovery requests and any other orders. And then they give us the answer. Or give us access and we go search them for the answer. And in this case, they gave us the answer. We relayed that to the Court.

...

MAJ Fein: Yes, your Honor, we did. And we were told that they were compiling the documents to do a damage assessment. We asked what is the status of the damage assessment so that we can relay it to the Court and this was the exact wording we were given.

...

MAJ Fein: ... We inquired into what documentation they had, that we could report on whether they have a draft damage assessment. And they reported back again, to date ONCIX has not produced any interim or final damage assessment in this matter, when we asked them the question.

...

MAJ Fein: So we did have discussions with both entities on what the differences could be, but at the end of the day we asked "do you have any documentation or do you have a damage assessment, and if not, what do you have?" And these were the responses that we were given and that we relayed to the Court.

Article 39(a) Audio Recording 6 June 2012.

45. MAJ Fein would have the Court believe that the conversations consisted of him constantly probing ONCIX, only to be met with a robotic and repeated: "ONCIX has not produced any

interim or final damage assessments in this matter.” Based on MAJ Fein’s version of events, there were at least three conversations about the issue of what ONCIX had. MAJ Fein would have the Court believe that the conversation went something like this:

MAJ Fein: We are calling to inquire as to what ONCIX has in terms of a damage assessment.

ONCIX: ONCIX has not produced any interim or final damage assessments in this matter.

MAJ Fein: I understand that. Can you tell me where you are in the process of working on the damage assessment?

ONCIX: ONCIX has not produced any interim or final damage assessments in this matter.

MAJ Fein: Even though you don’t have an interim assessment, do you have a draft?

ONCIX: ONCIX has not produced any interim or final damage assessments in this matter.

MAJ Fein: How about this – I understand what you don’t have. Can you tell me what you do have, so that we can relay that to the Court?

ONCIX: ONCIX has not produced any interim or final damage assessments in this matter.

MAJ Fein: Would it be correct to say that you are in the process of working on a draft damage assessment?

ONCIX: ONCIX has not produced any interim or final damage assessments in this matter.

Id.

46. The above hypothetical colloquy is intended to illustrate the absurdity of MAJ Fein’s latest representations to the Court that he had several (at least three) conversations with ONCIX and that “this was the exact wording [he was] given” time and again. *Id.* MAJ Fein states that he repeatedly probed into what ONCIX had, all to no avail (“We asked questions, we give them the relevant cases, the case law, we show them the discovery requests and any other orders.”; “We asked what is the status of the damage assessment so that we can relay it to the Court”; “We inquired into what documentation they had”; “We asked the questions and this is what we are given”; “but at the end of the day we asked “do you have any documentation or do you have a damage assessment, and if not, what do you have?”). *Id.* To believe the Government is to utterly disregard common sense and to suspend disbelief as to how normal conversations take place.

47. Even if it is true that ONCIX communicated nothing but that one sentence – “ONCIX has not produced any interim or final damage assessments in this matter” (apparently over and over again), a prosecutor is not permitted to blindly rely on such an assertion when he has knowledge to the contrary. At the very least, the Government had an obligation to say something to the Court to the effect, “We know that ONCIX is working on a damage assessment, but they have told us that they do not have any final or interim reports in this matter.” At that point, the Court

could have taken appropriate action (including, for instance, calling an ONCIX witness to discuss what ONCIX had or ordering the production of what ONCIX had).

48. The Government's parroting back of ONCIX's one-line statement casts serious doubts on other Government representations in this case. At this point, we do not know whether certain representations are based on first-hand knowledge of the Government, are based on unchallenged statements from other agencies, or are technically true but incomplete.

e) If the Government is to be Believed, ONCIX Completed a Draft Damage Assessment with Record Speed

49. The Government's story requires the Court to believe that from October 2010 until 21 March 2012, ONCIX did not have anything that would qualify as a draft or interim damage assessment. However, sometime between 21 March 2012 (when the Government made its representation that "ONCIX has not produced any interim or final damage assessments in this matter") and 17 May 2012, ONCIX created a draft damage assessment.

50. Otherwise stated, ONCIX did nothing with the information it had collected for nearly 18 months and then, in less than 2 months, created a draft damage assessment. As if that weren't enough, it planned on creating a final damage assessment by mid-July 2012. In short, the Government is representing that ONCIX had nothing for 18 months – and that 4 months later, ONCIX will have produced a final damage assessment.

51. This conflicts with the Government's account of how damage assessments are completed. At oral argument, MAJ Fein explained, "Damage assessment themselves are living documents that capture damage as the date of the document. It doesn't mean that damage can't happen the next day; which is why it is a very long process." Article 39(a) Audio Recording 15 March 2012 (unauthenticated record of trial at p. 165). As is clear from MAJ Fein's own words, damage assessments do not go from "zero" to "final" in a matter of four months.

52. Moreover, as pointed out by the Defense in oral argument, page 4 of DOS damage assessment shows that ONCIX did have a draft damage assessment at the time the Government made its representation to the Court. Additionally, the damage assessment completed by the Department of Homeland Security indicates that it is for ONCIX's damage assessment.⁶ Thus, either ONCIX is lying or the Government is lying.

f) The Government's Account of its Brady Obligations With Respect to the 63 Agencies Does Not Make Sense

53. On 23 February 2012, the Government represented at an 802 session and on the record that it had been conducting a *Brady* search for approximately a year and that it found no *Brady* material. Article 39(a) Audio Recording 23 February 2012, (unauthenticated record of trial at p.

⁶ As previously stated, the Defense was provided notification of the Department of Homeland Security's damage assessment for the first time on 8 June 2012. The Government has yet to provide notification to the Court.

39). It stated that it had searched different sub-agency files, even going so far as to the Department of Agriculture.⁷ In this respect, the Court stated:

MJ: The government advised the Court that although it has been extensively engaged in evaluating executive branch and sub-branch files for discoverable information prior to referral, the government's due diligence obligations under the *Brady Williams* case law; duty to find, evaluate and disclose favorable and material evidence to the defense will take additional time because of the need to cull through voluminous classified and unclassified information contained throughout executive branch [and] sub-branch agencies that have been involved in the classified information disclosure investigations.

Id. at p. 38.

54. The Defense added the following:

Mr. Coombs: Just that the when government spoke about its *Brady* search they stated at that time they had not found any *Brady* material even though they had looked for over a year.

Id. at p. 39.

55. The Court asked, "Is that correct?" to which MAJ Fein responded:

MAJ Fein: Your Honor, that is correct but also at the same time [we] stated that material continues to evolve because this is an on-going issue.

Id.

56. The Defense assumes that these sub-agencies that the Government represented it had been searching for a year prior to the February 2012 motions argument are the same 63 agencies that it refers to in Appellate Exhibit C.

57. The Government's latest admissions (below) prove that its previous statements about its *Brady* search were not truthful.

MAJ Fein: ... The NCIX as explained in the Government's filing to explain the difference between assessments and investigations. The NCIX is chartered to do a national level, national counterintelligence review – a damage assessment at a national level. That's what their – what the counter espionage act, excuse me, what the counterintelligence act set up. We briefed that in our filing. That is their charter. They do it government wide. They receive inputs from different government organizations. What Mr., excuse me, what the Defense has already

⁷ "Mr Coombs: Even going so far as going to the Department of Agriculture to see if they had potential information there. And then they stated; and they even state it here, that they have not found any *Brady* material." Transcript at p. 106.

referenced and we have already produced to the Defense are different entities that have submitted their information to NCIX. We have not reviewed any document that belongs to NCIX. Period. *What we have done is, we have gone to the originator, the owner of the information that was submitted to NCIX. The original entities, to request approval to review their material, and if discoverable, turn it over to the Defense. And that is what the Defense has been receiving.* Specifically, the ultimate source your Honor of these documents is not NCIX. The source of the documents that the Defense is receiving in discovery are the actual agencies. *So as mentioned earlier on the record today, the Department of Agriculture or the, or any of the executive departments that the Defense has received, those organizations independently did their own and submitted those.* We have gone to those agencies for efficiency purposes. We have acquired the documents, or attempting to finalize acquiring all of the documents. And then once we obtain them or review them get approval to turn them over if discoverable and give them to the Defense immediately once we get that approval.

...

MAJ Fein: Correct your Honor. It is our belief, at that point [February 2012], that they were compiling these other assessments *we knew about because we started reaching out once they told us about it – to go get those.* But, that they had no other documentation that would be subject to discovery – based off this response. So, yes we did know that their individual organizations were submitting theirs, and *that is why we went out to those independent organizations to get them approval and disclose them.*

Article 39(a) Audio Recording 6 June 2012 (emphases supplied).

58. As is clear from the above passages, MAJ Fein states he became aware that ONCIX had received inputs from various agencies in February 2012, and it was at that point that the Government began reaching out to these different agencies. (“we knew about [these other agencies] because we started reaching out once they told us about it – to go get those.”; “So as mentioned earlier on the record today, the Department of Agriculture or the, or any of the executive departments that the Defense has received, those organizations independently did their own and submitted those”). *Id.*

59. Indeed, this is confirmed in an email from SGT Bradley (a paralegal for the Government) to the EPA. SGT Bradley writes on February 27, 2012:

I am a paralegal for the prosecution team in the Court-Martial of Private First Class Bradley Manning in connection with “W#kileaks.” The purpose of this email is to request a copy of all documents your organization provided to NCIX approximately one year ago. Although we have been coordinating with NCIX/ODNI for the past year, just two weeks ago they determined that we cannot review copies of your organization’s documents in their possession, and we must directly go to your organization to coordinate a review. *See Attachment.*

60. It is clear that it wasn't until mid-February 2012 that the Government even began searching for *Brady* material from the 63 agencies. The search happened only because ONCIX told the Government that the Government could not "review copies of ... [various] organization's documents in [ONCIX's] possession" and must go to the original source of the documents.⁸ This begs the million dollar question: If the Government did not begin its search of the 63 agencies until mid-February 2012, how could the Government represent to the Court that it had *already* searched these same files in the year prior to referral? This simply does not make sense. The Government either did not search these files for the one-year prior to February 2012 (in which case, the Government will have misrepresented that it had conducted such a search) or the Government did search these files, but concluded that the information therein was not discoverable (in which case, this would reveal that: a) the Government did not understand the *Brady* standard at the time of the original search; and b) that the Government misrepresented when it learned of these other agencies' involvement). The Government's dates and representations simply do not line up and it should finally be held to account for its continued misrepresentations.

61. Moreover, SGT Bradley's email reveals that the Government had been "coordinating with NCIX/ODNI for the past year." *Id.* If this is the case, then the Government should have known what ONCIX had by way of a damage assessment. Moreover, how could the Government have been "coordinating" with ONCIX for a year and still not be reaching out to the individual agencies that provided inputs until February 2012? What was the Government doing for that year? Why did it take a year for the Government to figure out that they had to go back to the individual agencies for their respective damage assessments? None of this makes any sense.

g) The Letter from MAJ Fein to the General Counsel of ONCIX Demonstrates that The Government Did Not Just Learn of the ONCIX Draft on 17 May 2012

62. The letter from MAJ Fein to Ms. Tricia Wellman, the Deputy General Counsel at ODNI, reveals that the Government did not just learn that ONCIX had a draft damage assessment at the 17 May 2012 meeting as MAJ Fein suggests. MAJ Fein paints a picture where, after sharing the Court's 11 May 2012 ruling with ODNI/ONCIX, individuals at ONCIX determined that they did, in fact, have a draft damage assessment and convened a meeting with the Government to determine the way forward. If this was the case, the letter to Ms. Wellman would have read quite differently. It might have read something to the effect:

Ms. Wellman:

During the March 2012 motions argument and in subsequent emails to the Court, based on the input received from NCIX, the prosecution proffered to the Court

⁸ The Government says that it began searching the 63 agencies for damage assessments once ONCIX "told [the Government] about it" in the February timeframe. However, the Government also says "We have not reviewed any document that belongs to NCIX. Period." See Article 39(a) audio recording 6 June 2012. Presumably, this means that ONCIX gave the Government the list of the 63 agencies that had submitted damage assessments to ONCIX orally. Again, it is hard to believe that a representative from ONCIX would be on the phone with trial counsel, while the latter wrote down each and every one of the 63 agencies. More likely than not, the Government had seen a copy of the ONCIX damage assessment, or at least a copy of the list of agencies that ONCIX had contacted.

that NCIX had not completed any interim or final damage assessment. We have since learned, after a meeting on 17 May 2012, that NCIX does, in fact, have a draft damage assessment. Given this new information, we must inform the Court that NCIX does have a draft damage assessment. ...

63. Nowhere in the letter does MAJ Fein say that he has just learned that ONCIX has a draft damage assessment. Instead, he speaks about the “draft” as though he has known about it all along. See Appellate Exhibit CXIX, Letter from MAJ Fein to Ms. Wellman, 24 May 2012 (“the Court ruled that the Department of State’s damage assessment was discoverable, but did not rule on NCIX’s draft”; “based on the Court’s ruling, the previous discovery order, and applicable ethical obligations, the prosecution believes it must review NCIX’s draft damage assessment...”). In fact, MAJ Fein asks for access to “the *most recent* version of the [ONCIX] draft damage assessment” and asks ONCIX to “make the most recent draft available for review ... as soon as possible.” *Id.* This statement reveals that there are in fact, different versions of the draft damage assessment that MAJ Fein apparently just learned about. If a draft was just completed, how can it be that there are already multiple versions of it? If MAJ Fein had just learned that ONCIX had a draft damage assessment, he would have asked Ms. Wellman for “the draft damage assessment” not for “the most recent version of the draft damage assessment.”

* * *

64. The above facts, coupled with the Defense’s submissions in Appellate Exhibit CI (Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2; Defense Motion for Modified Relief); Appellate Exhibit CXX (Defense Response to Prosecution Notice to Court of ONCIX Damage Assessment) should reveal that things did not happen as the Government claims they did.

65. The Defense urges this Court to use Occam’s Razor⁹ – the simplest explanation is most likely the correct one. The simplest explanation here is the following: Both the Government and ONCIX knew that ONCIX had a draft damage assessment. The Government did not tell the Court this because the damage assessment is favorable to the accused and the Government believed that a draft damage assessment should not be discoverable. When the Court ruled *for the second time* that a draft damage assessment was indeed discoverable and the Defense filed its Motion to Compel Discovery #2, the Government realized it had to fess up to the Court about concealing the ONCIX damage assessment. This is, in reality, the most likely version of events – and the only version of events that does not require the Court to completely suspend common sense and better judgment.

II) The Government’s Latest Submission Does Not Refute Any of the Defense’s Allegations

⁹ “Occam’s razor is the law of parsimony, economy or succinctness. It is a principle urging one to select from among competing hypotheses that which makes the fewest assumptions and thereby offers the simplest explanation of the effect.” See http://en.wikipedia.org/wiki/Occam's_razor.

66. The Government's latest response says a whole lot of nothing. As indicated, the response does not even attempt to address any of the factual inconsistencies and issues raised by the Defense, including, but not limited to, the following:

- a) Why didn't the Government tell the Court about the ONCIX damage assessment?
- b) Why did the Government represent that it had searched the files of 63 agencies prior to February 2012 and found no *Brady*, but now is saying that it did not begin its *Brady* search until February 2012 after ONCIX informed the Government that it needed to go to these agencies?
- c) When did the Government learn of the FBI impact statement? (not when did it get approval to tell the Defense). When did the FBI begin the impact statement? When did it complete the impact statement?
- d) When did the Government learn of the Department of Homeland Security damage assessment? Why didn't the Government tell the Court about this at the 6 June 2012 motions argument, given that the parties and the Court were in the process of discussing what damage assessments existed?
- e) Why didn't the Government ever follow-up with HQDA? Why did it take someone at HQDA, nine months after the original memo was circulated, to realize that nobody had conducted a *Brady* search?
- f) Why hadn't the Government already searched the files of the Department of State? How can it be that two years into the case, the only document from the Department of State that the Government has seen is their Damage Assessment?
- g) Why has the Government not completed a *Brady* search of documents that it agrees are under military possession, custody and control?
- h) Why has the Government not yet completed a *Brady* search of closely aligned agencies?

67. Instead of answering these questions, or even one or two of these questions, the Government used the two-week extension by the Court to repeat what it has already said over and over again – that it understands *Brady* and it is working diligently to produce *Brady* discovery. The undisputed facts belie any assertion that the Government is being diligent in its *Brady* search. If it were, it would have answers to the questions outlined above.

68. Since the Government has not actually addressed the issue that it had indicated it would address, the Defense is instead left to respond to a slightly more robust argument that the Government has already made in its 24 May 2012 submission. *See* Appellate Exhibit C (Prosecution Response to Defense Motion to Compel Discovery #2). In this respect, the Defense would specifically like to address the following:

1. The Defense is not clear on why the Government is arguing in this motion that “the defense does not possess an unlimited right to discovery” and providing case citations to that effect. Government Response, p. 2-3. That is not what this motion is about. This motion is about whether the Government should be held to account for the steps it has taken in complying with discovery obligations. Thus, the Defense is unclear what the purpose of the discussion on pp. 2-3 is.

2. The Government is not correct when it states at p. 3 that “the defense does not have a right to discovery prior to referral under RCM 701 or *Brady*.” Under the military’s version of *Brady*, R.C.M. 701(a)(6), discovery must be produced “as soon as practicable” without reference to the date of referral. Other rules, including R.C.M. 701(a)(2) refer to “service of charges” as being the triggering date – but not R.C.M. 701(a)(6).
3. The Government’s statement on p. 3 that “the United States has disclosed more broadly than the rules of discovery require” is laughable. The Government states that “the prosecution disclosed FBI information regarding the accused’s travel and bank records that was not required to be produced under RCM 701(a)(6) nor *Brady*.” The Government here is referring to the fact that it provided these records as part of the FBI investigative file. The Defense estimates that approximately 90-95% of the file is redacted. There are pages upon pages of black in the file the Defense has received. To claim that the Government has gone “above and beyond” in producing travel and bank records (records which the accused *already has* because they are *his records*) is disingenuous to say the least.
4. The Government suggests at p. 4 that “[a]bsent misconduct, a *Brady* violation does not occur until the completion of trial” though it concedes that “misconduct, including gamesmanship, constitutes a *Brady* violation no matter the timing.” The Government is getting caught up again in the wrong issue. For the purposes of this motion, the Defense is seeking an accounting for the Government’s due diligence obligations because things simply “do not add up.” Whether we call it a “*Brady* violation” or something else doesn’t really matter. However, the Defense would submit that a failure to conduct a diligent *Brady* search would constitute a *Brady*/discovery violation.
5. The Government states at p. 4, “Here, the Court found neither prosecutorial misconduct nor a discovery or a *Brady* violation.” The Defense submits that, in light of the evidence at the time, the Court’s ruling was very generous and gave the Government the benefit of the doubt. Many events have come to light *after* the Court’s ruling in March 2012 (e.g. the lack of diligence with respect to the Department of State; the ONCIX damage assessment; the FBI impact statement; the HQDA memo). The Government cannot continue to rely on the Court’s ruling from three months ago to shield it from current scrutiny.
6. The Government seems to suggest that the Defense does not have the right to call the Government to task for its *Brady* failures because the Defense is concurrently raising motions to further the interests of PFC Manning. *See* p. 4 (“Still, the defense raises anew complaints of the timing of discovery without regard to the motions it has submitted to the Court.”). To the extent that this is the implication of the Government’s statement, it is preposterous. A Defense counsel is entitled to do everything to advance the interests of his client; indeed, if he does not, he may be subject to a claim for ineffective assistance of counsel. To suggest that the Defense should not complain about the timing of discovery because it, itself, is raising critical motions is absurd.

7. The Government has once again misrepresented the Defense's argument regarding R.C.M. 701(a)(6). See p. 4. Despite clarifying this for the Government no less than three or four times, the Government still believes that the Defense is saying that "federal agencies ... are military authorities under RCM 701(a)(2)." For the fifth time, the Defense's argument is that files belonging to agencies that are closely aligned with the Government in this case are in the "possession, custody or control" of military authorities for the purposes of R.C.M. 701(a)(6). The Government refers to this claim as "novel" and "unorthodox." It is not novel or unorthodox. It is the law in federal court – and the Defense submits, it is the law in military courts as well.
8. The Government makes a convoluted argument at p. 5 ("Citing the prosecution's legal arguments twenty-five times, the Defense improperly equates discovery litigation with an alleged discovery violation. ... However, despite the numerous citations to prosecution responses, the defense does not explain how a statement of the prosecution's steps in complying with its obligations under Brady and RCM 701(a)(6) would alleviate the allegations conjured by the defense. Indeed, the defense attempts to make prosecution responses to defense motions the basis of its motion requesting unprecedented relief without explaining how the relief will cure the hypothetical prejudice that has not occurred."). First, how is the Defense to know what the Government is doing with respect to discovery absent using the Government's responses? Second, it self-evident how a due diligence accounting would "alleviate the allegations conjured by the defense." If the Government provides an accounting, the Court and Defense will know what is being searched and not searched, and how we should proceed from here.
69. Moreover, the Government requests that, should an accounting be ordered, it be permitted to file the accounting *ex parte*. The Court should not permit an *ex parte* due diligence filing by the Government. Answering questions about the steps it has taken in discovery does not implicate attorney work-product. Indeed, the Government has already provided sample letters sent to various agencies, examples of the specific requests that were made, and the dates on which certain requests were made.
70. The Defense believes that the Government's attempt to account for its diligence *ex parte* is an attempt to protect it from scrutiny by the Defense. To date, it has been the Defense that has alerted the Court to the numerous and varied problems in the Government's submissions such as, the Government's use of the words "alleged", "completed" and "unaware"; the Government's citing of the federal appellate standard for *Brady*; the Government's obfuscation with respect to the difference between a "damage assessment" and an "investigation"; the Government's failure to follow-up on the HQDA memo etc. By providing a due diligence accounting to the Court *ex parte*, the Government may be more inclined to take liberties with the truth, because there is no one but the Military Judge to challenge the Government.¹⁰
71. The Defense submits that if, for whatever reason, there is a limited portion of the due diligence accounting that is classified, the Government should redact that portion and the

¹⁰ It is ironic that the Government is requesting to submit a due diligence statement *ex parte*, while citing *United States v. Bumgarner*, 49 C.M.R. 770, 772 (A.C.M.R. 1974) for proposition that "objecting" is essential to "maintain[ing] the adversarial system."

Military Judge should decide whether that portion should be provided for the Defense. At the end of the day, if the Government has nothing to hide, it should not be afraid to account to Defense, the Court and the public at large for all the steps it has taken in this proceeding.

72. The Defense believes that 30 days is an unreasonably long period of time to chronicle its due diligence efforts. The purpose of such an accounting is so that the Court and the Defense know what is still outstanding and can proceed accordingly (e.g. by ordering certain files to be searched, etc.). In fact, the request for 30 days to provide a statement of its due diligence itself speaks volumes about the slow pace of discovery and lack of diligence of the Government. If the Government has been keeping track of what it is doing, there is no reason it should not be prepared to provide the accounting in a matter of *days*.

73. The Defense submits that the following passage from *United States v. Chapman*, 524 F.3d 1073 (9th Cir. 2008), wherein the Ninth Circuit affirmed the district court's decision to dismiss the indictment due to reckless violations of the government's discovery obligations, is apposite:

Here, although the case involved hundreds of thousands of pages of discovery, the AUSA failed to keep a log indicating disclosed and nondisclosed materials. The AUSA repeatedly represented to the court that he had fully complied with *Brady* and *Giglio*, when he knew full well that he could not verify these claims. When the district court finally asked the AUSA to produce verification of the required disclosures, he attempted to paper over his mistake, offering "in an abundance of caution" to make new copies "rather than find the record of what we turned over." Only when the court insisted on proof of disclosure did the AUSA acknowledge that no record of compliance even existed. Finally, the dates on many of the subsequently disclosed documents post-date the beginning of trial, so the government eventually had to concede that it had failed to disclose material documents relevant to impeachment of witnesses who had already testified. In this case, the failure to produce documents and to record what had or had not been disclosed, along with the affirmative misrepresentations to the court of full compliance, support the district court's finding of "flagrant" prosecutorial misconduct even if the documents themselves were not intentionally withheld from the defense. We note as particularly relevant the fact that the government received several indications, both before and during trial, that there were problems with its discovery production and yet it did nothing to ensure it had provided full disclosure until the trial court insisted it produce verification of such after numerous complaints from the defense.

Id. at 1085. There are several important things about this passage. First, the court indicates that a diligent prosecutor would have kept logs or records of discovery; thus, a prosecutor would not require 30 days to disclose such information to the court. Second, *Chapman* provides precedent for a court to require a prosecutor to provide a due diligence accounting when it becomes clear that there are issues with discovery. Third, it is interesting that the prosecutors in *Chapman* who were found to have committed discovery violations used the two of the same expressions that the Government is so fond of using ("we understand and are complying with *Brady*" and "in an abundance of caution").

74. Finally, the Government apparently has not thought very carefully about its request that any delay be attributable to the Defense for speedy trial purposes.¹¹ If the Court orders the Government to conduct a due diligence accounting, it is because the Court believes that *something is not be right* in the discovery process. In such circumstances, how can the delay then be attributable to the Defense for speedy trial purposes?

75. In short, the Court should regard the Government lack of candor in its latest submission as revelatory. After the Court expressed serious concerns about the ONCIX damage assessment at the last motions argument, one would think that the Government would be direct and forthright with the Court at this point about certain key issues such as the FBI impact statement, the HQDA memo, etc. The fact that the Government hasn't been forthright – and instead insists that it will not provide any details absent a Court order tells us that something is very wrong with the discovery in this court-martial.

CONCLUSION

76. For all the reasons stated herein¹² the Defense moves for the Court to order the Government to provide a due diligence accounting of the steps it has taken to comply with its *Brady* obligations.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

¹¹ This is illustrative of the numerous nonsensical positions the Government takes in this litigation. For instance, the Defense requested witnesses from ONCIX, the FBI and DHS in support of the 25 June 2012 motions argument. The Government opposed on the basis that this was a new issue that should be litigated in July, *after the motions argument in which the witnesses would have testified*. In the Government's zeal to oppose any Defense request or motion, the Government has lost all common sense.

¹² as well as the reasons stated in Appellate Exhibit XCVI (Defense Motion to Compel Discovery #2); Appellate Exhibit XCVIII (Defense Reply to Government Response to Motion to Compel Discovery #2); Appellate Exhibit XCIX (Supplement to Defense Motion to Compel Discovery #2); Appellate Exhibit CI (Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2; Defense Motion for Modified Relief); Appellate Exhibit CXX (Defense Response to Prosecution Notice to Court of ONCIX Damage Assessment); and the Defense's filings of 18 June 2012 and 21 June 2012 requesting witnesses for the purpose of this motion)

ATTACHMENT

Bradley, Princeton L. SGT USA JFHQ-NCR/MDW SJA

From: [REDACTED]
Sent: Friday, March 02, 2012 12:54 PM
To: Bradley, Princeton L. SGT USA JFHQ-NCR/MDW SJA
Cc: [REDACTED]
Subject: Re: Request to Review NCIX Response (UNCLASSIFIED)

Sergeant Bradley:

EPA has no documents to provide to the Department of the Army, per your request, below.

Approximately one year ago, after reviewing approximately 2400 documents, EPA determined that there were no EPA documents that were problematic and needed to be reported and provided to NCIX. EPA informed this to NCIX in an informal, oral communication.

[REDACTED]

From: "Bradley, Princeton L. SGT USA JFHQ-NCR/MDW SJA"
<princeton.bradley@afhqncr.mdtm.mil>

To: [REDACTED]
Cc: [REDACTED]

Date: 02/27/2012 04:52 PM
Subject: Request to Review NCIX Response (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: FOUO

Ma'am,

Good afternoon, I hope that you are well. I am a paralegal for the prosecution team in the Court-Martial of Private First Class Bradley Manning in connection with "Wikileaks." The purpose of this email is to request a copy of all documents that your organization provided to NCIX approximately one year ago. Although we have been coordinating with NCIX/ODNI for the past year, just two weeks ago they determined that we cannot review copies of your organization's documents in their possession, and we must directly go to your organization to coordinate a review.

We are requesting this information to determine if there is any information that may be discoverable and may require production by the government. None of the information will leave our office, unless your organization has approved its release, and it will remain classified at all times.

We would like to review the documents from your organization as soon as possible. This short suspense is necessary as the accused was arraigned last week, and to allow for enough time to coordinate with your organization, if information is discoverable. If the information is classified, please feel free to use the lead prosecutor's SIPRNET and JWICS email addresses below to transmit your documents. If you would like to speak with me, please call at 202-685-1975 and if you would like to speak with our lead prosecutor, please call Captain Ashden Fein at 202-685-4572.

SIPRNET: ashden.fairchild@hqnorthcom.smil.mil
JWICS: ashden.fairchild@hqnorthcom.smil.mil

Thank you.

Very Respectfully,
Princeton Bradley
Sergeant, U.S. Army
Paralegal Non-Commissioned Officer
Military Justice, OSJA
Fort McNair
202-685-4489 / 1975
princeton.bradley@hqnorthcom.smil.mil

Classification: UNCLASSIFIED
Caveats: FOUO

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE REQUESTED
INSTRUCTION: ARTICLE 92
AND SPECIFICATION 1 OF
CHARGE II**

DATED: 22 June 2012

1. The Defense requests the Court issue the standard Military Judges Benchbook instructions for the Article 92 offense in Charge III.
2. The Defense requests the following instructions to be given to the panel regarding Specification 1 of Charge II:

Court Instructions

In Specification 1 and Charge II, the accused is charged with the offense of disorders and neglects to the prejudice of good order and discipline or of a nature to bring discredit upon the armed forces, a violation of Article 134, UCMJ. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following two (2) elements:

- (1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, wrongfully and wantonly cause to be published on the internet intelligence belonging to the United States government, having knowledge that intelligence published on the internet is accessible to the enemy; and
- (2) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

Authority: Article 134, UCMJ, 10 U.S.C. § 934; Military Judges Benchbook, DA Pam 27-9, para. 3-60-2A.

Court Definitions

(1) Wrongfully and Wantonly Cause to be Published on the Internet

The first element that the government must prove beyond a reasonable doubt is that the accused wrongfully and wantonly caused to be published on the Internet intelligence belonging to the United States.

“Wrongful” or “wrongfully” means without legal justification or excuse.

“Wanton” or “wantonly” includes “recklessness” but may connote willfulness, or a disregard of probable consequences, and thus describes a more aggravated offense.

A person causes intelligence to be published on the Internet when the person personally publishes the intelligence on the Internet or knowingly or intentionally induces or sets in motion acts by an animate or inanimate agency or instrumentality which result in the publication of the intelligence on the Internet.

If you find that the accused did not wrongfully and wantonly cause intelligence to be published on the Internet, you must find the accused not guilty of this offense.

Authority: Article 134, UCMJ, 10 U.S.C. § 934; Military Judges Benchbook, DA Pam 27-9, para. 3-60-2A; MCM, Part IV, para. 1.b(2)(a); *id.*, Part IV, para. 35.c(8) (defining “wanton” for purposes of Article 111); *id.*, Part IV, para. 100a.c(4) (defining “wanton” for purposes of Article 134, offense of “reckless endangerment”).

(2) Knowledge that Intelligence Published on the Internet is Accessible to the Enemy

The second element that the government must prove beyond a reasonable doubt is that the accused had knowledge that information published on the Internet would be accessible to the enemy.

This element requires that the accused actually knew that information published on the Internet would be accessible to the enemy. That is, actual knowledge on the part of the accused is required, and constructive knowledge is insufficient. In other words, this element is not satisfied if you find only that the accused should have known that information published on the Internet would be accessible to the enemy, but that the accused did not actually know this fact.

If you find that the accused did not actually know that information published on the Internet would be accessible to the enemy, you must find the accused not guilty. An accused’s mistake as to this fact, no matter how unreasonable, is a complete defense to this offense, so long as the mistake was genuine.

Authority: Appellate Exhibit LXXX, at 5 (explaining that one of the elements of Specification 1 of Charge II is “that the accused *knew* that intelligence published on the internet is accessible to the enemy”); *United States v. Nix*, 29 C.M.R. 507, 511 (C.M.A. 1960); *United States v. Walters*, 28 C.M.R. 164, 167 (C.M.A. 1959) (“[W]here subjective knowledge is required, reasonableness is not one of the criteria which should be used in instructing on mistake of law or fact.”).

(3) Conduct prejudicial to good order and discipline

With respect to “prejudice to good order and discipline,” the law recognizes that almost any irregular or improper act on the part of a service member could be regarded as prejudicial in some indirect or remote sense; however, only those acts in which the prejudice is reasonably

direct and palpable is punishable under this Article.

With respect to “service discrediting,” the law recognizes that almost any irregular or improper act on the part of a service member could be regarded as service discrediting in some indirect or remote sense; however, only those acts which would have a tendency to bring the service into disrepute or which tend to lower it in public esteem are punishable under this Article.

Not every act of publishing intelligence belonging to the United States government on the Internet constitutes an offense under the UCMJ. The government must prove beyond a reasonable doubt, either by direct evidence or by inference, that the accused’s conduct was prejudicial to good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces. In resolving this issue, you should consider all the facts and circumstances to include the effect, if any, upon the accused’s or another’s ability to perform his/her/their duties; the effect the conduct may have had upon the morale or efficiency of a military unit; the harm, if any, to the United States or the unit from the alleged disclosures.

If you find that the accused’s conduct was not prejudicial to good order and discipline and/or was not of a nature to bring discredit upon the armed forces, you must find the accused not guilty.

Authority: Article 134, UCMJ, 10 U.S.C. § 934; Military Judges Benchbook, DA Pam 27-9, para. 3-60-2A; *United States v. Mayo*, 12 MJ 286 (C.M.A. 1982); *United States v. Perez*, 33 MJ 1050 (A.C.M.R. 1991); *United States v. Sellars*, 5 MJ 814 (A.C.M.R. 1977).

Maximum Punishment

3. Rule for Courts-Martial (R.C.M.) 1003(c)(1)(B)(i) provides:

For an offense not listed in Part IV of this Manual which is included in or closely related to an offense listed therein the maximum punishment shall be that of the offense listed; however, if an offense not listed is included in a listed offense, and is closely related to another or is equally related to two or more listed offenses, the maximum punishment shall be the same as the least severe of the listed offenses.

R.C.M. 1003(c)(1)(B)(i).

4. The Defense submits the charged specification is closely related to a violation of Article 92 for failure to obey a regulation, AR 380-5. First, Specification 1 of Charge II and a violation of AR 380-5 have similar mens rea requirements: the charged specification requires that an accused act wrongfully and wantonly (including reckless, willfulness, or a disregard of probable consequences), and AR 380-5 punishes one who “knowingly, willfully, or negligently” discloses covered information, AR 380-5, para. 1-21(a). Second, the intelligence information covered by Specification 1 of Charge II is likely within the definitions of “classified information” or “sensitive information” contained in AR 380-5. Finally, the conduct underlying the offense alleged in the charged specification is closely related to the conduct that would constitute a violation of AR 380-5: the disclosure of information to an unauthorized person entity. An

Article 92 failure to obey a regulation carries a two-year maximum confinement. So too does the offense alleged in Specification 1 of Charge II.

5. Although the Government has alleged knowledge on the part of PFC Manning that intelligence published on the Internet is accessible to the enemy, this does not rise to the knowledge required by Article 104, aiding the enemy. The knowledge required for Specification 1 of Charge II – knowledge that information on the Internet could be accessed by an enemy – is far removed from the knowledge required for the Article 104 offense – “actual knowledge by the accused that he was giving intelligence to the enemy.” Appellate Exhibit LXXXI, at 2. Therefore, Specification 1 of Charge II is not closely related to a violation of Article 104. Moreover, a capital offense may not be tried under Article 134. *see* 10 U.S.C. § 934, and Article 104 provides for capital punishment, *see id.* § 904 (providing that any person who violates the section “shall suffer death or such other punishment as a court-martial or military commission may direct.”). Thus, the Article 104 offense cannot be considered in determining what offenses are “closely related” under R.C.M. 1003(c)(1)(B)(i).

6. The Defense respectfully requests the above instructions and definitions be given by the Court.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

RULING:
DELAY OF COURT'S RULING
ON DEFENSE MOTION TO
COMPEL DISCOVERY #2

DATED: 8 June 2012

The Government has requested thirty (30) days to delay the Court's ruling on the Defense Motion to Compel Discovery #2 in order to search for the records concerning the Department of State requested by the defense in its Addendum to Defense Motion to Compel Discovery #2. The defense does not object to this request.

Factual Findings:

1. On 7 June 2012, three Department of State witnesses, specifically Ms. Marguerite Coffey, Ms. Rena Bitter, and Ms. Catherine Brown, testified during a motions hearing in the above captioned courts-martial. The witnesses referenced the below records in their testimony. The witnesses testified that they were unaware whether the below records remain in existence.

(1) written assessments produced by the Chiefs of Mission used to formulate a portion of the draft damage assessment completed in August of 2011;

(2); written Situational Reports produced by the WikiLeaks Working Group between roughly 28 November 2010 and 17 December 2010;

(3) written minutes and agendas of meetings by the Mitigation Team;

(4) Information Memorandum for the Secretary of State produced by the WikiLeaks Persons at Risk Group;

(5) a matrix produced by the WikiLeaks Persons at Risk Group to track identified individuals;

(6) formal guidance produced by the WikiLeaks Persons at Risk Group and provided to all embassies, including authorized actions for any identified person at risk;

(7) information collected by the Director of the Office of Counterintelligence within the Department of State (DoS) regarding any possible impact from the disclosure of diplomatic cables; and

(8) any prepared written statements for the DoS's reporting to Congress on 7 and 9 December 2010.

2. On 7 June 2012, the Government requested the Court delay the Court's ruling for thirty (30) days on the Defense Motion to Compel Discovery #2, for information pertaining to the Department of State, in order to search for the above referenced records.

3. On 7 June 2012, the defense submitted its Addendum to Defense Motion to Compel Discovery #2 and requested the above records. The defense requested that the prosecution produce this material under Rule for Courts-Martial (RCM) 701(a)(2) or, in the alternative, RCM 703. The defense also requested that the prosecution produce this material under RCM 701(a)(6).

ORDER:

1. The Government will **immediately** begin the process of searching for and inspecting the following information:

(1) written assessments produced by the Chiefs of Mission used to formulate a portion of the draft damage assessment completed in August of 2011;

(2) written Situational Reports produced by the WikiLeaks Working Group between roughly 28 November 2010 and 17 December 2010;

(3) written minutes and agendas of meetings by the Mitigation Team;

(4) Information Memorandum for the Secretary of State produced by the WikiLeaks Persons at Risk Group;

(5) a matrix produced by the WikiLeaks Persons at Risk Group to track identified individuals;


(6) formal guidance produced by the WikiLeaks Persons at Risk Group and provided to all embassies, including authorized actions for any identified person at risk;

(7) information collected by the Director of the Office of Counterintelligence within the Department of State (DoS) regarding any possible impact from the disclosure of diplomatic cables; and

(8) any prepared written statements for the DoS's reporting to Congress on 7 and 9 December 2010.

2. By **8 July 2012**, the Government shall **notify** the Court which of the above records exist and, for those records that do exist, file a supplemental response to the Defense's Motion to Compel Discovery #2.

So **ORDERED** this 8th day of June 2012.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

UNITED STATES

y.

MANNING, Bradley E., PFC
U.S. Army, [REDACTED]
Headquarters and Headquarters Company,
U.S. Army Garrison, Joint Base Myer-
Henderson Hall, Fort Myer, VA 22211

**RULING: DEFENSE MOTION-
CLARIFICATION OF RULING
MOTION TO COMPEL
DISCOVERY 2**

DATED: 25 June 2012

1. On 23 June 2012, this Court issues a Ruling re: Defense Motion to Compel Discovery #2. The Defense moved for clarification of the ruling. Both parties request the Court to decide this issue at today's article 39(a) session.
2. The Court's order applies to files the Government has previously reviewed and files the Government will review.
3. In its Motions to Compel Discovery, Defense proffered that the discovery is necessary for the Defense to accurately assess the damage that the alleged leaks caused. As such, the Court ordered the Government to disclose information from files subject to RCM 701(a)(2) that involve investigation, damage, and mitigation measures. The law requires the Government to disclose information obviously material to the preparation of the defense. Material means relevant and helpful to the defense. Thus, the Government in reviewing files subject to RCM 701(a)(2) will provide the Defense any information beyond the investigation, damage, and mitigation measures that are obviously relevant and helpful to the defense.

Q10

DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)
U.S. Army, [REDACTED])
Headquarters and Headquarters Company,)
U.S. Army Garrison, Joint Base Myer-)
Henderson Hall, Fort Myer, VA 22211)

**RULING: DEFENSE MOTION-
DUE DILIGENCE**

DATED: 25 June 2012

1. On 10 May 2012, as part of its Motion to Compel Discovery, Defense moved this court to suspend the proceedings for several weeks and require the Government to state with specificity the steps it has taken to comply with its obligation to disclose information favorable to the defense IAW RCM 701(a)(6). Defense further moved the Court to grant a 2-3 month continuance after receipt of completed discovery until the start of trial. On 29, 30, and 31 May 2012, and on 7 June 2012, Defense submitted additional filings to the Court on this issue, expanding its request that the Court suspend the proceedings and require the Government to state with specificity the steps it has taken to comply with its discovery obligations under RCM 701(a)(2), 701(a)(6), and 905(b)(4). The Government opposes.

2. Defense moves the Court to require the Government to answer the following questions:

(1) What agencies (63) has the Government contacted to conduct a *Brady* Review? Has the Government attempted to contact all agencies, to include: (Interagency Committee Review) (President's Intelligence Advisory Board, House of Representatives Oversight Committee) to conduct a *Brady* review?

(2) When did the Government make its inquiry?

(3) How many documents did the Government review?

(4) What were the results of the Government review?

(5) What did the Government ask of these agencies?

3. Defense further moves the Court to require the Government to turn over *Brady* material or state there is no *Brady* information from the following files: CID, DIA, DISA, CENTCOM and SOUTHCOM, FBI, DSS, DOS, DOJ, Government Agency, ODNI, ONCIX.

4. Defense provided the Court with a 17 April 2012 Memorandum for Principal Officials of HQDA stated that "it was only recently determined that no action had been taken by HQDA

pursuant to the 29 July 2011 memorandum from DOD OGC to HQDA requesting it to task Principal Officials to search for, and preserve, any discoverable information.

The Law: The Court has authority to order the Government to provide a due diligence statement IAW RCM 701(g)(1).

Conclusions of Law:

1. Since referral, there have been 2 broad Defense motions to compel discovery IAW RCM 701(a)(2) and RCM 701(a)(6) for information from the files of multiple DoD agencies, aligned government agencies, non-aligned government agencies, Interagency Committee Review, President's Intelligence Advisory Board, and House of Representative Oversight Committee.
2. This is a complex case involving multiple government agencies and entities. The Court is not clear what identifiable files pertaining to PFC Manning relevant to this case are maintained by the various agencies (including but not limited to those referenced in paragraph (3) above), what inquiries the Government has made to discover the existence of agency files pertaining to PFC Manning, when the Government became aware of the existence of particular agency files, and what files the Government has examined under RCM 701(a)(6)/*Brady* and/or RCM 701(a)(2).
3. This Court must rule upon the motions to compel discovery that have been filed in this case and a speedy trial motion to be filed by the Defense. One document containing the information in paragraph (2) above will assist the Court in addressing discovery and speedy trial issues arising during this trial.
4. The Court makes no findings of lack of due diligence by the Government. Both parties will have an opportunity to litigate the due diligence of the Government in providing discovery during the speedy trial motion.
5. By **25 July 2012**, the Government will provide the Court with a statement of due diligence, in the format attached, stating:
 - a. Steps the Government has taken to inquire about the existence of files pertaining to PFC Manning from Government agencies/entities;
 - b. When these inquiries were made;
 - c. When the Government became aware of the existence of each file pertaining to PFC Manning from Government agencies/entities;
 - d. What files the Government has searched for *Brady*/RCM 701(a)(6) information and when;
 - e. What files the Government has searched for information material to the preparation of the defense IAW RCM 701(a)(2) and when.
 - f. What information from the above files the Government has disclosed to the Defense;
 - g. What files the Government has reviewed and found no discoverable information;
 - h. What files the Government has decided not to disclose to the Defense;
 - i. What files the Government has identified that have yet to be searched for *Brady*/RCM 701(a)(6) and/or RCM 701(a)(2).

6. By **25 July 2012**, the Government will provide a timeline and synopsis of the inquiries and communications between the Government and ONCIX.

7. The filing by the Government will be *ex parte* to the Court. The Government will identify what classified filings have not been identified to the Defense.

8. The Court will not suspend the proceedings pending the Government response. The case calendar will continue into July and August with scheduled motions that are not impacted by receipt of defense discovery. At the July 2012 Article 39(a) session, the case calendar will be revised to reflect Article 39(a) sessions after August at the 6 week schedule reflected in the current scheduling order.

9. The Court will grant a reasonable continuance to the Defense upon receipt of compelled discovery to prepare their case.

The Defense Motion for Due Diligence Filing is **GRANTED** in part as set forth above.

So **ORDERED**: this 25th day of June 2012.

A handwritten signature in black ink, appearing to read 'DRL', is positioned above the printed name of the signatory.

DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit

Appellate Exhibit 178

7 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 178

Enclosure 1

75 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 178

Enclosure 2

15 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 178

Enclosure 3

8 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 178

Enclosure 4

22 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 178

Enclosure 5

16 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 178,
Enclosure 6
has been entered into
the record as
Prosecution Exhibit 63

Appellate Exhibit 178,
Enclosure 7
has been entered into
the record as
Prosecution Exhibit 64

Appellate Exhibit 178

Enclosure 8

3 pages and 1 CD

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 178,
Enclosure 9
has been entered into
the record as
Prosecution Exhibit 152

Appellate Exhibit 178

Enclosure 10

3 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 179

1 page

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

DEFENSE UPDATED CASE
CALENDAR

DATED: 27 June 2012

1. The Court is currently scheduling Article 39(a) sessions with the following default schedule at the request of the parties: two weeks for parties to file motions; two weeks for parties to file responses; five days for parties to file replies (although replies are not necessary for Phase 6); and one week for the Court to review all pleadings before the start of the motions hearing.

a. Phase 1. Immediate Action (21 February 2012 - 16 March 2012)

b. Phase 2(a). Legal Motions excluding Evidentiary Issues (29 March 2012 - 26 April 2012)

c. Phase 2(b). Legal Motions (10 May 2012 - 8 June 2012)

d. Pretrial Motions (27 July 2012 – 8 August 2012)

e. Phase 3a. Evidentiary Issues (22 June 2012 - 20 July 2012)

- (A) Filing: 22 June 2012
- (B) Response: 6 July 2012
- (C) Reply: 11 July 2012
- (D) Article 39(a): 16-20 July 2012

(1) **Government Initial Witness List**

- (A) Filing: 22 June 2012

(2) **Proposed Members Instructions for All Charged Offenses**

(3) **Witness Lists for Article 13**

- (A) Defense Witness Lists: 6 July 2012
- (B) Government Objections (if any): 10 July 2012
- (C) Defense Motion to Compel (if any): 13 July 2012

(4) **Preliminary Determinations on Admissibility¹**

(5) **Defense Motion to Dismiss All Charged Offenses under 18 U.S.C. 1030(a)(1) #2**

¹ The Government plans on moving to pre-admit evidence that has MRE 902(11) attestations.

- (6) **Maximum Punishment for Lesser Included Offenses**
- (7) **Government Motion for Substitutions under MRE 505(g)(2) for FBI Impact Statement**
- (8) **Government Motion for Modification of Court Order: Government Motion: Protective Order(s) dated 24 April 2012**
- (9) **Proposed Questionnaires**
(A) Filing: 6 July 2012
(B) Response: 11 July 2012
(C) Reply: N/A
- (10) **Defense 505(h)(3) Notice for Charged Documents**
(A) Filing: 6 July 2012
(B) Response: 11 July 2012
(C) Reply: N/A
- (11) **Disclosure of Any Records from the Department of State and for those Records that Exist, Government filing of a Supplemental Response to Defense's Motions to Compel Discovery #2**
(A) Filing: 9 July 2012²
- (12) **Defense Motion to Compel Discovery #2 (Department of State Material)³**
(A) Filing: 7 June 2012
(B) Response: 9 July 2012
(C) Reply: 11 July 2012
- (13) **Defense Motion to Compel Discovery #2 (FBI Investigative File and Impact Statement)⁴**
- (14) **Government will review the ONCIX Damage Assessment by 13 July 2012 and Notify the Court Whether the Government Anticipates ONCIX Will Seek Limited Disclosure IAW MRE 505(g)(2) or Claim a Privilege IAW MRE 505(c)**
(A) Filing: 20 July 2012

² The Government will indicate whether it will seek limited disclosure IAW MRE 505(g)(2) or claim a privilege IAW MRE 505(c).

³ See Appellate Exhibit CXLII.

⁴ In compliance with the Court's Order, the Government will immediately begin the process of producing the FBI investigative file and impact statement IAW RCM 703(f)(4)(A). The Government will comply with the 20 July 2012 (notice of limited disclosure or claim of privilege), 25 July 2012 (notice of *in camera* proceeding), and 3 August 2012 filing dates for the FBI investigative file and impact statement.

(15) Notification to the Court Whether the Government Anticipates any Government Entity that is Subject of Defense Motion to Compel #2 Will Seek Limited Disclosure IAW MRE 505(g)(2) or Claim a Privilege IAW MRE 505(c)

(A) Filing: 20 July 2012

(16) Notification to the Court Whether the Government Anticipates any Government Entity for RCM 701(a)(6)/*Brady* Information and/or RCM 701(a)(2) Material to the Preparation of the Defense Information that is Not Subject to Defense's Motions to Compel Discovery #1 or #2, Will Seek Limited Disclosure IAW MRE 505(g)(2) or Claim a Privilege IAW MRE 505(c)

(A) Filing: 20 July 2012

(17) If Any Relevant Agency Claims a Privilege (Including ONCIX) Under MRE 505(c), and Government Seeks an *In Camera* Proceeding under MRE 505(i), Government Will Move for an *In Camera* Proceeding IAW MRE 505(i)(2) and (3) and Provide Notice to Defense IAW MRE 505(i)(4)(A).

(A) Filing: 25 July 2012

(18) Government's Due Diligence Statement to the Court

(A) Filing: 25 July 2012

f. Phase 4. Mini-Article 39(a) Session (27 July 2012 – 8 August 2012)

(A) Filing: 27 July 2012

(B) Response: 3 August 2012

(C) Article 39(a): 10 August 2012 (If needed)

(1) Updated Proposed Case Calendar

g. Phase 4. Pretrial Motions (27 July 2012 – 31 August 2012)

(A) Filing: 3 August 2012

(B) Response: 17 August 2012

(C) Reply: 22 August 2012

(D) Article 39(a): 27-31 August 2012

(1) Article 13

(A) Filing: 27 July 2012⁵

(2) Motions *in Limine* (Government 404(b) motion and additional Government motions to preclude)

(3) Motions to Suppress

⁵ The Defense agreed to the filing date of one week earlier to give the United States the necessary time to respond.

(4) For all Files under the Possession, Custody, or Control of Military Authorities Where a Privilege under MRE 505(c) is Not Claimed, the Government Will Immediately Disclose to the Defense, or Submit them to the Court for an *In Camera* Review under RCM 701(g) or for Limited Disclosure under MRE 505(g)(2). This Includes the Documents Collected Based Upon the 17 April 2012 HQDA Memorandum.⁶

(A) Filing: 3 August 2012

(5) For all FBI/DSS Files where a Privilege under MRE 505(c) is Not Claimed, the Government Will Immediately Disclose to the Defense, or Submit them to the Court for an *In Camera* Review under RCM 701(g) or for Limited Disclosure under MRE 505(g)(2).

(A) Filing: 3 August 2012

(6) For all DOS Files where a Privilege under MRE 505(c) is Not Claimed, the Government Will Immediately Disclose to the Defense, or Submit them to the Court for an *In Camera* Review under RCM 701(g) or for Limited Disclosure under MRE 505(g)(2).

(A) Filing: 3 August 2012

(7) For all *Brady* Information Subject to Defense's Motions to Compel Discovery #1 and #2, where a Privilege under MRE 505(c) is Not Claimed, the Government Will Immediately Disclose to the Defense, or Submit them to the Court for an *In Camera* Review under RCM 701(g) or for Limited Disclosure under MRE 505(g)(2).

(A) Filing: 3 August 2012

(8) For all RCM 701(a)(6)/*Brady* Information and/or RCM 701(a)(2) Material to the Preparation of the Defense Information that is Not Subject to Defense's Motions to Compel Discovery #1 or #2, where a Privilege under MRE 505(c) is Not Claimed, the Government Will Immediately Disclose to the Defense, or Submit them to the Court for an *In Camera* Review under RCM 701(g) or for Limited Disclosure under MRE 505(g)(2).

(A) Filing: 3 August 2012

(9) For the ONCIX Damage Assessment where a Privilege under MRE 505(c) is Not Claimed, the Government Will Immediately Disclose to the Defense, or Submit it to the Court for an *In Camera* Review under RCM 701(g) or for Limited Disclosure under MRE 505(g)(2).

(A) Filing: 3 August 2012

(10) Government Shall Disclose All Evidence that it will Introduce on the Merits and During Sentencing.

(A) Filing: 3 August 2012

(11) Witness Lists for Speedy Trial

⁶ This refers to documents involving investigation, damage assessment or mitigation measures as well as all documents *beyond* those that involve investigation, damage assessment or mitigation measures, that are material to the preparation of the defense and in the possession, custody and control of military authorities (e.g. DA, DIA, DISA, SOUTHCOM, CENTCOM, CYBERCOM, HQDA).

- (A) Defense Witness Lists: 3 August 2012
- (B) Government Objections (if any): 17 August 2012
- (C) Defense Motion to Compel (if any): 22 August 2012

(12) Defense 505(h)(3) Notice for Damage Assessments and Other Classified Information Provided on 3 August 2012⁷

- (A) Filing: 17 August 2012
- (B) Response: 22 August 2012
- (C) Reply: N/A

(13) Requests for Judicial Notice

(14) Defense Production of Government Reciprocal Discovery Request

- (A) Date: 27 August 2012

h. Phase 5. Mini-Article 39(a) (7 September 2012 – 19 September 2012)

- (A) Filing: 7 September 2012
- (B) Response: 14 September 2012
- (C) Article 39(a): 19 September 2012 (If needed)

(1) Updated Proposed Case Calendar

(2) Government Motion to Compel Discovery (if any)

- (A) Filing: 7 September 2012
- (B) Response: 14 September 2012

i. Phase 5. Pretrial Motions (7 September 2012 – 19 October 2012)

- (A) Filing: 14 September 2012
- (B) Response: 28 September 2012
- (C) Reply: 5 October 2012
- (D) Article 39(a): 15-19 October 2012

(1) Speedy Trial, including Article 10

- (A) Filing: 7 September 2012⁸

(2) Production of Compelled Discovery for Government Motion to Compel Discovery (if any)

- (A) Date: 17 September 2012

⁷ This notice is for all material that the Government produced by 3 August 2012 to the Defense. If the Government proposes summaries that are not acceptable to the Court, and additional time is needed, the Defense will file a supplemental 505(h)(3) notice seven days after receiving the Court approved summaries under M.R.E. 505(g)(2).

⁸ The Defense agreed to the filing date of one week earlier to give the United States the necessary time to respond.

(3) Defense Witness List

- (A) Filing: 21 September 2012
- (B) Government Objection to Defense Witnesses: 28 September 2012
- (C) Motion to Compel Production: 3 October 2012
- (D) Response: 8 October 2012

(4) Defense Notice of its Intent to Offer the Defense of Alibi, Innocent Ingestion, or Lack of Mental Responsibility IAW RCM 701(b)(2)

(5) Defense Notice of Accused's Forum Selection and Notice of Pleas in Writing

- (A) Filing: 7 September 2012

(6) Government Supplemental Witness List⁹

- (A) Filing: 10 October 2012

(7) Litigation Concerning MRE 505(h) and MRE 505(i)

- (A) Filing: 7 September 2012
- (B) Response: 14 September 2012

j. Phase 6. Pretrial Motions (3 October 2012 – 26 October 2012)

- (A) Filing: 3 October 2012
- (B) Response: 17 October 2012
- (C) Article 39(a): 25-26 October 2012

(1) Pre-Qualify Government Experts

(2) Pre-Qualify Defense Experts

(3) *Grunden* Hearing for All Classified Information

(4) Voir Dire Questions, Flyer, Findings/Sentence Worksheet, All CMCOs

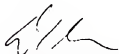
- (A) Filing for Court Review: 10 October 2012

⁹ The United States stated that it will submit a supplemental witness list based solely on any rulings from the Government Motion to Compel Discovery and any disclosures by the Defense after the 21 September 2012 witness list due date. Thus, the Government's filing on 22 June 2012 should represent a good faith listing of the Government's witnesses for the merits and sentencing phases absent any compelled discovery from the Defense or disclosures by the Defense after submission of the Defense's witness list. Accordingly, any witness added should clearly be based upon the Defense's Witness List, Defense disclosures, or Court Rulings.

k. **Trial by Members (1 November 2012 – 20 November 2012)**

(A) Voir Dire: 1-2 November 2012

(B) Trial: 5 – 20 November 2012



DAVID E. COOMBS
Civilian Defense Counsel

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

**DEFENSE REQUESTED
WITNESSES: ARTICLE 13
MOTION**

MANNING, Bradley E., PFC)

U.S. Army, [REDACTED])

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

DATED: 3 July 2012

1. On behalf of PFC Bradley E. Manning, his civilian counsel, David E. Coombs requests the attendance of the following witnesses for purpose of his Article 13 motion:

- a) CAPT William J. Hocker, Fort Belvoir, william.j.hocker.mil@health.mil, (571) 231-1350. CAPT Hocker will be out of the office until at least 10 July 2012. He will testify that neither the Quantico Brig Commander, CW4 James Averhart, nor the Security Battalion Commander, Col. Robert Oltman, gave him any reasons for maintaining the Prevention of Injury (POI) precautions other than stating it was for PFC Manning's safety. He will testify that Col. Oltman intimated that he was receiving instruction from a higher authority on the matter, but did not say who was providing this direction. Capt. Hocker will testify that he knew that the higher base authorities had frequent (sometimes weekly) meetings to discuss PFC Manning. Capt. Hocker will testify that he gave weekly status reports stating that he felt the POI precautions were unnecessary. Capt. Hocker will testify that he recalls a meeting with Col. Oltman where Col. Oltman stated that PFC Manning would remain in his current status Maximum Custody and POI status unless and until he received instructions from higher authority to the contrary. Capt. Hocker cannot recall Col. Oltman's exact words, but he does recall that Col. Oltman saying something to the effect of "I will not have anything happen to Manning on my watch. So, nothing is going to change in his custody status. He won't be able to hurt himself and he won't be able to get away, and our way of making sure of that is that he will remain on Maximum Custody and POI indefinitely." Capt. Hocker will testify that he expressed concern to Col. Oltman because he did not feel there was a behavioral health reason for the POI. In response, he will testify that Col. Oltman said "We will do whatever we want to do. You make a recommendation and then I have to make a decision based upon everything else." He will also testify that Col. Oltman made it clear that nothing would change with PFC Manning regardless of his behavior or the recommendations of behavioral health.
- b) COL Rick Malone, Chief, Walter Reed Forensic Psychiatry Service, rick.malone@us.army.mil, (202) 567-0057 – (703) 588-1288. He will be out of the office until the end of July. He will testify that the Quantico Brig instituted more precautions than he would from a psychiatric perspective. He will testify that he consistently recommended to the Quantico Brig to remove PFC Manning from POI

status. He will testify that if PFC Manning were not in custody, he would have recommended routine outpatient care for him. He will testify that it has long been known that restriction of environmental and social stimulation has a negative effect on mental function. He will testify that PFC Manning's restrictive confinement was not necessary from a psychiatric perspective, and that he made repeated recommendations that the PFC Manning's status should be downgraded.

- c) CAPT Kevin D. Moore, Walter Reed National Military Medical Center, (703) 784-1779, kevin.d.moore@med.navy.mil (former Defense expert provided by the Government). He will testify that during a meeting in early January of 2011, the Security Battalion Commander in charge of the Quantico Brig, Col. Robert Oltman, clearly stated to the Brig Staff that "I will not have anything happen to Manning on my watch.... So, nothing is going to change.... He won't be able to hurt himself and he won't be able to get away, and our way of making sure of that is that is he will remain on Maximum Custody and POI indefinitely." He will testify that one of the other Brig psychiatrists, Capt. William Hocter then said "You know Sir, I am concerned because if you are going to do that, maybe you want to call it something else because it is not based upon anything from behavioral health." In response, Capt. Moore will testify that Col. Oltman said "We will do whatever we want to do. You make a recommendation and then I have to make a decision based upon everything else." Capt. Moore will testify that Capt. Hocter then said, "Well then don't say it is based upon mental health. You can say it is Maximum Custody, and just don't put that we [behavioral health] are somehow involved in this." Col. Oltman replied, "Well, that is what we are going to do." Capt. Moore will testify that a Command Judge Advocate was present during the meeting, but did not intercede to say that Col. Oltman was in the wrong. Capt. Moore will also testify that he spoke with others at the Brig to see if they knew why the Brig was so heavy handed on PFC Manning. He will testify that others at the Brig told him that they have never seen anything like this before. Capt. Moore will testify that others told him that they were afraid to speak out about the situation given the concern of what would happen to them as a result of any complaint about PFC Manning's treatment.
- d) Col. Robert G. Oltman, Security Battalion Commander, robert.g.oltman@usmc.mil, (703) 784-3730. Col. Oltman will be out of the office until 3 August 2012. He will testify concerning PFC Manning confinement conditions and his Maximum Custody and POI status. He can also testify regarding any outside influence concerning the custody status of PFC Manning.
- e) LCDR David Moulton, Former Associate Program Director, National Capital Consortium Psychiatry Residency Program, Walter Reed National Military Medical Center. LCDR Moulton has now left active duty and is in the reserves. He can be reached at University Neuropsychiatric Institute, 501 Chipeta Way, Salt Lake City, Utah, david.moulton@hsc.utah.edu, (240) 246-4201. He will testify concerning the effects of solitary confinement on the psychological well-being of those subjected to it, and PFC Manning specifically. He will testify that isolation or solitary confinement is among the most harmful conditions that can be imposed upon a detainee. He will also testify how PFC Manning was held in restrictive solitary confinement for nearly a year without any

psychiatric or behavioral justification. Finally, he will testify how these conditions likely placed PFC Manning at an increased risk of exacerbating any existing psychiatric symptomatology or condition.

- f) LTC Dawn Hilton, Commander, Fort Leavenworth Joint Regional Correctional Facility, dawn.l.hilton@us.army.mil, (913) 758-4503. She will testify that once PFC Manning was transferred to the JRCF on 19 April 2011, he spent nine days in the normal indoctrination process. After completing the indoctrination process, PFC Manning was held in medium custody with all privileges of a normal pretrial detainee. She will testify that PFC Manning was not placed upon any POI status given the fact there was no psychiatric or behavioral health basis for such a status. Since being held in that medium custody status, PFC Manning has not engaged in any self-harm behavior, engaged in any assaultive behavior towards the guards, or made any attempt to escape from custody.
- g) Mr. Juan Méndez, U.N. Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Visiting Professor, Washington College of Law, 4801 Massachusetts Ave., NW, Washington, DC 20016, (202) 274-4252, jmendez@wcl.american.edu. Mr. Méndez will testify about his communications with the U.S. Government regarding the confinement conditions of PFC Manning. He will testify that he was told the confinement conditions were imposed on account of the seriousness of the offenses. He will also testify that the U.S. Government informed him that PFC Manning was not being held in "solitary confinement" but was being held in "prevention of harm watch" but would not offer any details about what harm was being prevented by such a status. He will also testify regarding his efforts to meet with PFC Manning for an unmonitored conversation. Despite his numerous requests, he will testify that he was informed that his conversation would be monitored. Mr. Méndez will testify that the U.S. Government's refusal to allow unmonitored conversations with PFC Manning violate international norms and U.N. requirements. Due to the U.S. Government's refusal to allow unmonitored conversations, Mr. Méndez had to decline the opportunity to meet with PFC Manning.
- h) PFC Bradley Manning, Headquarters and Headquarters Company, U.S. Army Garrison, Joint Base Myer-Henderson Hall, Fort Myer, VA 22211. He will testify for the limited purposes of the motion under M.R.E. 104(d) and M.R.E. 304(f). PFC Manning will testify concerning his nine months of unlawful pretrial punishment that he endured while at Quantico.

2. The Defense also requests that the Government produce the following physical pieces of evidence under R.C.M. 703(f)(4)(A) for purposes of the motion:

- a) The Quantico issued suicide prevention smock;
- b) the Quantico issued suicide prevention blanket; and
- c) the Quantico issued suicide prevention bed that was issued to PFC Manning while at the Quantico Confinement Facility.

3. The Defense reserves the right to supplement this witness list should it be necessary to do so. If the Defense submits any additional request for witnesses, it will do so in a timely manner.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', is positioned above the printed name.

DAVID EDWARD COOMBS
Civilian Defense Counsel

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

)
)
) **DEFENSE RESPONSE TO**
) **GOVERNMENT MOTION FOR**
) **AUTHORIZATION OF A**
) **SUBSTITUTION FOR FBI**
) **IMPACT STATEMENT**

) DATED: 6 July 2012
)

RELIEF REQUESTED

1. The Defense requests that this Court find that the FBI Impact Statement is material to the preparation of the defense and Order that it be produced to the Defense under RCM 703(f). Alternatively, the Defense requests that the Court deny any proposed substitutions where, considering the mindset of Defense counsel (including the questions referenced herein), the Court concludes that the classified information itself is necessary to enable the accused to prepare for trial.

EVIDENCE

2. The Defense does not request any witnesses for this motion, but does request that the Court consider Appellate Exhibit IX, XXXVI, CXVI, CXLVI, and CXLVII for the purposes of this motion.

FACTS

3. The FBI has not claimed a privilege under MRE 505(c). Therefore, the damage assessment being considered by the Court is governed by *Brady*/R.C.M. 701(a)(6), R.C.M. 703(f), and M.R.E. 505(g)(2).

4. The Court has found that the FBI is "closely aligned" with the Government in this case. Appellate Exhibit XXXVI, p. 11.

ARGUMENT

A. The *In Camera* Standard

5. The Government's non-*ex parte* filing requests the Court to approve of its redacted information within the original FBI impact statement. The government maintains that "the information contained within the original report, which is redacted, does not meet the RCM 702(a)(6) or *Brady/Giglio* standards and therefore is not discoverable, nor it is material to the preparation of the defense or relevant and necessary for production under RCM 703(f)." Government In Camera Motion for Authorization of a Substitution of the FBI Impact Statement under MRE 505(g)(2), p. 2.

6. In the case at hand, the FBI is an agency that participated in a joint investigation in this case. The Government has a due diligence duty to search for discoverable information under *Brady* and RCM 701. The Government must search not only its own files but (1) the files of law enforcement authorities that have participated in the investigation of the subject matter of the charged offenses; (2) investigative files in a related case maintained by an entity closely aligned with the prosecution, and (3) other files as designated in a defense discovery request that involved a specified type of information within a specified entity. *Brady v. Maryland*, 373 U.S. 83 (1963); RCM 701.

7. As the Court noted, RCM 701 and RCM 703 work together "when production of evidence not in the control of military authorities is relevant and necessary for discovery." Appellate Exhibit XXXVI, p. 9, citing *United States v. Graner*, 69 M.J. 104 (C.A.A.F. 2010). Under RCM 703(f), the burden is on the Defense to show the production of evidence outside the control of military authorities is relevant and necessary. RCM 703(f). "Evidence that is material to the preparation of the defense under the control of other government agencies can be relevant and necessary for discovery, requiring production of the evidence from the other government entities pursuant to RCM 703(f)(1) and (4)(A)." Appellate Exhibit CXLVII, p. 5. The Court determined that it would "review the FBI Impact Statement *in camera* to determine whether it is material to the preparation of the defense to the extent relevant and necessary to require production for disclosure." Appellate Exhibit CXLVII, p. 6.

8. As previously stated, "material to the preparation of the defense" is not a difficult standard to satisfy. In *United States v. Cano*, 2004 WL 5863050 at *3 (A. Crim. Ct. App. 2004), our superior court discussed the content of the "materiality" standard under R.C.M. 701(a)(2)(A):

In reviewing AE V *in camera*, the military judge said that he examined the records and AE III contained "everything . . . [he] thought was even remotely potentially helpful to the defense." That would be a fair trial standard, but our examination finds a great deal more that should have been disclosed as "material to the preparation of the defense." We caution trial judges who review such bodies of evidence *in camera* to do so with an eye and mind-set of a defense counsel at the beginning of case preparation. That is, not solely with a view to the presentation of evidence at trial, but to actually preparing to defend a client, so that the mandate of Article 46, UCMJ, is satisfied.

See also *United States v. Roberts*, 59 M.J. 323, 326 (C.A.A.F. 2004) (“The defense had a right to this information because it was relevant to SA M’s credibility and was therefore material to the preparation of the defense for purposes of the Government’s obligation to disclose under R.C.M. 701(a)(2)(A).”) (emphasis added); *United States v. Adens*, 56 M.J. 724, 733 (A.C.C.A. 2002) (“We respectfully disagree with our sister court’s narrow interpretation that the term ‘material to the preparation of the defense’ in R.C.M. 701(a)(2)(A) and (B) is limited to exculpatory evidence under the *Brady* line of cases and hold that our sister court’s decision in *Trimper* should no longer be followed in Army courts-martial. There is no language in R.C.M. 701, or in its analysis, indicating any intent by the President to limit disclosure under Article 46, UCMJ, to constitutionally required exculpatory matters. As noted above, R.C.M. 701 is specifically intended to provide ‘for broader discovery than is required in Federal practice’ (R.C.M. 701 Analysis, at A21–32), and unquestionably is intended to implement an independent statutory right to discovery under Article 46, UCMJ.”); *United States v. Webb*, 66 M.J. 89, 92 (C.A.A.F. 2008) (“[U]pon request of the defense, the trial counsel must permit the defense to inspect any documents within the custody, or control of military authorities that are ‘material to the preparation of the defense.’ R.C.M. 701(a)(2)(A). Thus, an accused’s right to discovery is not limited to evidence that would be known to be admissible at trial. It includes materials that would assist the defense in formulating a defense strategy.”).

9. Thus, if the Court determines the information from the FBI Impact Statement is material to the preparation of the Defense, then it is relevant and necessary to require production under RCM 703(f). So, the first step in the Court’s analysis must be whether the FBI Impact Statement contains *Brady* and whether it contains information that is material to the preparation of the defense – as in “helpful” to the preparation of the defense so as to require its production under RCM 703(f).

B. The Proposed Substitution

10. Once the Court has determined what information in the FBI Impact Statement would qualify as being either *Brady* or material to the preparation to the Defense, then the Court must examine the proposed substitution with a view to determining whether the classified information is itself necessary to enable the accused to prepare for trial. *United States v. Lonetree*, 31 M.J. 849 (N-M-C.M.R. 1990), aff’d 35 M.J. 396 (C.M.A. 1992).

11. Limited disclosure and substitutes under MRE 505(g)(2) include:

- a) Deletion of specific items of classified information from documents to be made available to an accused;
- b) Substitution of a portion or summary of the information for such documents; and
- c) Substitution of a statement admitting relevant facts.

All of these are permitted unless the judge determines that the classified information itself is necessary to enable the accused to prepare for trial. See M.R.E. 505(g)(2).¹

¹ MRE 505(g)(2) provides as follows: “Limited disclosure. The military judge, upon motion of the Government, shall authorize (A) the deletion of specified items of classified information from documents to be made available to

12. Thus, the Government is authorized under M.R.E. 505(g)(2) to substitute a summary of the information contained in a classified document rather than the classified document. The rule itself recognizes, however, that the Court may recognize that "disclosure of the classified information itself is necessary to enable the accused to prepare for trial." This deference to the accused's rights even after a claim of privilege by the government is well-settled. See *United States v. Rezaq*, 134 F.3d 1121 (D.C. Cir. 1998)(holding that a trial court considering substitutions "...should, of course, err on the side of protecting the interests of the defendant").

13. In making the determination as to whether the classified information is "necessary to enable the accused to prepare for trial," the Defense requests that this Court consider the following factors adopted by the Court in Appellate Exhibit CXLVI:

- a) What is the extent of the redactions/substitutions?
- b) Has the Government narrowly tailored the substitutions to protect a Governmental interest that has been clearly and specifically articulated?
- c) Does the substitution provide the Defense with the ability to follow-up on leads that the original document would have provided?
- d) Do the substitutions accurately capture the information within the original document?
- e) Is the classified evidence necessary to rebut an element of the 22 charged offenses, bearing in mind the Government's very broad reading of many of these offenses?
- f) Does the summary strip away the Defense's ability to accurately portray the nature of the charged leaks?
- g) Do the substitutions prevent the Defense from fully examining witnesses?
- h) Do the substitutions prevent the Defense from exploring all viable avenues for impeachment?
- i) Does the Government intend to use any of the information from the damage assessments? If so, is this information limited to the summarized document provided by the Government? If the information intended to be used by the Government is not limited to the summarized document, does the Defense in fairness need to receive the classified portions of the documents to put the Government's evidence in proper context?
- j) Does the original classified evidence present a more compelling sentencing case than the proposed substitutions by the Government?
- k) Do the proposed substitutions prevent the Defense from learning names of potential witnesses?
- l) Do the substitutions make sense, such that the Defense will be able to understand the context?
- m) Is the original classified evidence necessary to help the Defense in formulating defense strategy and making important litigation decisions in the case?

the defendant, (B) the substitution of a portion or summary of the information for such classified documents, or (C) the substitution of a statement admitting relevant facts that the classified information would tend to prove, unless the military judge determines that disclosure of the classified information itself is necessary to enable the accused to prepare for trial. The Government's motion and any materials submitted in support thereof shall, upon request of the Government, be considered by the military judge in camera and shall not be disclosed to the accused."

- n) Is it unfair that the Government had access to the unclassified version of the damage assessment and the Defense did not? Does that provide a tactical advantage to the Government?

CONCLUSION

14. Accordingly, the Defense requests that this Court find that the FBI Impact Statement is material to the preparation of the defense and Order that it be produced to the Defense under RCM 703(f). Alternatively, the Defense requests that the Court deny any proposed substitutions where, considering the mindset of Defense counsel (including the questions referenced herein), the Court concludes that the classified information itself is necessary to enable the accused to prepare for trial.

Respectfully submitted,



DAVID E. COOMBS
Civilian Defense Counsel

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, [REDACTED])

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

**DEFENSE RESPONSE TO
GOVERNMENT MOTION
FOR MODIFICATION OF
PROTECTIVE ORDER**

DATED: 6 July 2012

RELIEF SOUGHT

1. The Defense requests that this Court deny the Government's motion for modification of the current protective order to the extent that the Government submits that the Defense should now be permitted to redact and post filings unilaterally. The Defense will voluntarily agree to redact an individual's job title or position if that individual is not a party to the trial and only one individual holds that job title or position.

WITNESSES/EVIDENCE

2. The Defense would request the Court to consider the following Attachments:

- a) Attachment A: 23 March 2012 Email from MAJ Fein to the Court;
- b) Attachment B: 2 April 2012 Email from MAJ Fein to the Court;
- c) Attachment C: 2 April 2012 Email from the Court to MAJ Fein;
- d) Attachment D: 29 March 2012 Email from Mr. Coombs to MAJ Fein;
- e) Attachment E: 29 March 2012 Email from MAJ Fein to Mr. Coombs;
- f) Attachment F: 5 April 2012 Email from MAJ Fein to Mr. Coombs;
- g) Attachment G: 16 April 2012 Email from MAJ Fein to Mr. Coombs;
- h) Attachment H: 14 March 2012 Email from Mr. Coombs to MAJ Fein; and
- i) Attachment I: 30 May 2012 Email Exchange between Mr. Coombs and MAJ Fein.

FACTS

3. When the Defense first notified the Court that it intended to publish its motions on the internet, the Government strenuously opposed. On 23 March 2012, MAJ Fein sent the following email to the Court:

Ma'am,

The United States opposes the defense's request to freely publish all motions, responses, and replies on the Internet. The defense's request would act to publicize information provided to the defense in discovery, the public disclosure of which may require outside agency approval and the substance of which may cause irreparable prejudice to the United States. Much of the information in this case was disclosed under various protective orders which remain in effect, including grand jury subpoena information, Secretary of the Army 15-6 investigation information, and law enforcement sensitive information. This protected information was provided to the defense for discovery and under the specific condition not to publish or release it outside of the specific individuals who were allowed access to the information.

The defense purports that it wants to publish this information online to keep the public informed of the proceeding. The public, however, is already well informed of the proceedings. The public was present at the Article 32 hearing, the arraignment, and the first motions hearing, and will continue to be present at all open portions of the motions hearings and the trial. The command provided the theater next door for overflow area so that the public can freely watch the proceedings and the media operations center for the media. Additionally, other than the electronic filing process, the military justice system is more open than the federal system from the Article 32 proceedings through the end of the trial.

The United States does not intend to publish its pleadings online. If the defense remains intent on publishing all pleadings and their enclosures online, the United States requests the opportunity to file a motion for a protective order or multiple protective orders under RCM 701(g)(2) and 806(d) for the Court to regulate the defense's use of information gained through discovery. Additionally the United States requests the Court allow the prosecution thirty days to receive input from all the different federal entities on what information they provided for discovery which they did not intend to be made publically available. The sole purpose of discovery is to prepare for trial. Motions are filed to shape legal issues and belong to the Court. Most motions, e.g., motions to suppress or exclude evidence or testimony, are not appropriate for publication. Freely publicizing all pleadings, at this stage of the proceedings, may undermine the effectiveness of the publicity order and will circumvent those measures adopted to regulate what is available to the public and significantly jeopardize many interests of the United States, to include, protecting classified information (in the case of a spillage), preserving the confidentiality of law enforcement information, preventing potential witnesses from receiving information outside the scope of their projected testimony, protecting testifying witnesses, protecting trial participant safety, protecting the personal information of potential panel members, preventing disclosure of government information that threatens national security and is unclassified, and the deliberative processes of the United States Government. Furthermore, the United States believes that the defense's intended course of action would result in

a substantial likelihood of materially prejudicing the proceeding, in violation of, inter alia, RCM806(d) and Army Regulation 27-26, specifically Rule 3.6.

See Attachment A.

4. Prior to a final protective order being in place, the Defense published a synopsis of the upcoming motions arguments on Mr. Coombs' blog. The blog contained a general description of the types of issues that would be litigated. MAJ Fein objected to the Defense's blog post and on 2 April 2012 wrote to the Court:

Ma'am,

Good morning. Could you please clarify a portion of your interim order (Government Request for Leave to File Protective Order(s))? It was the government's understanding that we would have an opportunity to redact and/or object to the defense posting the Defense filings or proposed filings before the defense posts the information to the internet. Although the defense has not posted its actual filings or proposed filings, the defense has posted information that speaks directly to the substance of its proposed filings: "...if the redacted motions are not available, the following will provide a general understanding of what Defense motions are being addressed on April 24th through 26th...." The entire posting is attached for your reference.

It is the government's understanding that the defense's posting of a summary of its motions violates the Court's interim order in that the government did not have the opportunity to object to this information prior to its posting. Although we have not had an opportunity to check with the different equity holders, there does not appear to be any information that we would otherwise protect in THIS posting. This action seems to be an attempt by the defense to bypass the procedures that the Court ordered. The prosecution's ultimate concern is that the defense is picking and choosing what it thinks is appropriate for disclosure, which does not allow the United States to review the material. It is the government's duty to protect individuals and information, ensure the integrity of the process and a fair trial, which includes protecting overly prejudicial information, as well as unclassified but protected and classified information.

Could you please provide clarification on what the defense is authorized to post and whether the government will have the opportunity to review the information prior to posting?

See Attachment B.

5. The Court dismissed MAJ Fein's concerns, stating "The intent of the interim order was to ensure no information was published outside of court that included information from discovery via protective order, information subject to privilege under MRE 505 and 506, and PII to protect

witness/participant privacy and safety. The interim order was not intended to prevent the defense from publishing their legal theory for upcoming motions." *See* Attachment C.

6. Prior to beginning its redactions, the Defense emailed the Government to get the Government's position on what information needed to be redacted. The Defense wrote on 29 March 2012:

I am in the process of conducting my redactions. I would like to get the Government's position on whether you would have any objection to the following:

- a) Quoting statements by Government counsel during arguments;
- b) Quoting from Government Pleadings;
- c) Quoting emails from the Government to the Court and/or the Defense; and
- d) Quoting Court Rulings.

See Attachment D.

7. The Government responded, "The government has no objection to a and d below because those are matters of public record, so long as they are accurate. Depending on what is written in b and c, the government might have an objection." The Government provided no further elaboration on this statement. *See* Attachment E.

8. On 5 April 2012, MAJ Fein wrote to the Defense (copying the Court) and stated:

In order to make this process more efficient, the United States recommends that you submit the documents to us with see-through redaction boxes (or colored highlights) so all parties can read the information behind the redaction and the documents can be more easily reviewed by the prosecution and any relevant federal entity. After our review, we will return the document with proposed redaction boxes (or colored highlights). For this first round, we will recreate your redactions on a clean document with redaction boxes, so the process can continue moving forward quickly and efficiently.

See Attachment F. The Defense complied with the Government's request and has since highlighted all proposed redactions in yellow to facilitate the review by the Government. Because many of the motions are purely legal, they have not required any redactions.

9. Since April 2012, the Defense has made redactions in utmost good faith – and has in fact redacted more than it considers necessary so as to avoid any litigation over the issue. The Government has not once expressed any concerns with the Defense's redactions.

ARGUMENT

10. The Defense does not understand how the Government can go from its position in April 2012 ("The defense's request would act to publicize information provided to the defense in discovery, ... the substance of which may cause irreparable prejudice to the United States.") to its position today ("The prosecution requests that the Court allow the defense to publish subsequent court filings or proposed filings upon certifying with the Court that such filings do not contain any unredacted protected information").

11. In early April, the Government was concerned about the parade of horrors that would befall the proceeding and the United States if the Defense were to publish its motions publicly:

Freely publicizing all pleadings, at this stage of the proceedings, may undermine the effectiveness of the publicity order and will circumvent those measures adopted to regulate what is available to the public and significantly jeopardize many interests of the United States, to include, protecting classified information (in the case of a spillage), preserving the confidentiality of law enforcement information, preventing potential witnesses from receiving information outside the scope of their projected testimony, protecting testifying witnesses, protecting trial participant safety, protecting the personal information of potential panel members, preventing disclosure of government information that threatens national security and is unclassified, and the deliberative processes of the United States Government. Furthermore, the United States believes that the defense's intended course of action would result in a substantial likelihood of materially prejudicing the proceeding.

See Attachment A. In fact, the Government was so concerned about all these bad things happening that it requested thirty days to review a given Defense filing. *Id.* Apparently, the Government is not concerned about any of these things anymore and is prepared to risk "irreparable prejudice to the United States" and "materially prejudicing the proceeding" simply because the process of reviewing the redactions has gotten "overly burdensome." See Appellate Exhibit CLXIII at p. 3.

12. In April 2012, MAJ Fein stated that "It is the *government's* duty to protect individuals and information, ensure the integrity of the process and a fair trial, which includes protecting overly prejudicial information, as well as unclassified but protected and classified information." See Attachment B. Apparently, the Government is prepared to abdicate that duty because it's just too hard on them.

13. Prior to addressing the substance of the Government's motion, the Defense submits that the current motion shows the hypocrisy of the Government's litigation positions in this case. The Government often makes the-world-will-end-if-this-happens arguments, undermining the Government's credibility in the eyes of the Court and the public at large. For instance, the Government argued that the Defense should have to prepare all of its motions (classified and unclassified) from a trailer on Fort Meade – any other order would compromise national security and cause grave danger to the United States. This latest motion shows just how much credence the Court should give to these types of arguments.

14. First and foremost, the Government's position simply does not make sense. The Government states that it is required to "coordinate the approval" of Defense filings with various equity holders. See Appellate Exhibit CLXIII, p. 2 ("Since the applicable Court Order on 24 April 2012, the defense has submitted filings outside the schedule detailed by the existing case calendar, requiring the prosecution and the proper agencies, without notice, to coordinate the approval of such unexpected filings"; "Given the number of agencies involved, reviewing the defense filings requires the prosecution to identify the referenced agencies, submit such filings to those agencies, and coordinate with the proper representatives for approval or necessary redactions.")). However, the Government is prepared to cede responsibility for the motions and allow the Defense to review/redact/file motions on its own. This obviously means that *it is not necessary to have equity-holders' approval* in order to review and publish the motions. In other words, if the Government is now prepared to allow the Defense to post its motions unilaterally, then the Government is undertaking a wholly unnecessary process in getting approvals from various agencies. It is hard to believe that the Government does not see the fatal flaw in its own argument – it is asking the Court to relieve it from an obligation (consulting with equity holders and getting approvals) that it does not actually have. If agency approval is not necessary, why can't a team of five Government lawyers review a document, which they have to read anyway, and make the determination on their own as to whether anything contained therein is problematic?

15. The Government's excuse for no longer wanting to be subject to the protective order *that it requested* is that the process has become "overly burdensome." See Appellate Exhibit CLXIII, p. 3. The Government says that "[f]or the prosecution, such a requirement disrupts its preparation for upcoming Article 39(a) sessions and its continued effort to ensure the accused receives a fair and speedy trial." *Id.* The Defense submits that with a prosecution team the size of a starting football lineup, the Government should be able to keep on track of redactions (conveniently highlighted in yellow) *and* prepare for argument *and* ensure the accused gets a fair trial.

16. The Government then complains that the process is "overly burdensome ... [for] the United States Government as a whole." *Id.* The Government already tried a variation of this argument with respect to producing a witness from the Department of State; the Court did not buy it then, nor should it buy it now.

17. What is troublesome is the Government's next sentence. The Government states, "[f]or the United States Government organizations and agencies, such a requirement disrupts on-going operations and ultimately stalls its support to the court-martial process relating to pretrial and trial matters, *including obtaining information and requisite approvals in discovery.*" See Appellate Exhibit CLXIII at p. 3 (emphasis added). To the Defense, this looks like a not-so-veiled threat: If you make us continue with reviewing redactions, we will slow down your discovery.

18. This is not the first time the Government has resorted to subtle threats. When the Court ordered the Government to review the hard drives of the computers for certain specified programs, the Government decided at the last-minute it would rather turn over the hard drives

¹ The Court's reaction to this over-the-top argument was, "It's one witness, MAJ Fein."

than produce to the Defense the results of the forensic searches ordered by the Court. The Defense opposed and asked the Government to produce the forensic searches as per the Court's timeline, as well as the computer hard drives. MAJ Fein implied that if the Defense did not agree to waive the forensic results, it would take much longer for the Defense to get access to the hard-drives. In this respect, MAJ Fein stated:

As for the forensic drives, CID will continue examining the drives as per the Court's order and we will provide the results by 20 April 2012. *However, in an effort to save time and resources for all parties involved (defense, government computer experts, government classification experts), we can produce the forensic images of the drives, as per the defense's original request.* The defense will be able to conduct any analysis/procedure it wishes with complete copies of the drives.

We can wait until after 20 April 2012, however it will take more time after that to get those drives fully reviewed for security classification purposes, than merely the filenames. If the defense ultimately wants the forensic images and access to the files (as per the original motion and the renewed motion) sooner than later, the United States recommends the defense support this way forward, so we can divert CID resources from continuing to search for these programs and having to dedicate security experts to the review of the lists, and just have all of them focus on the actual files.

See Attachment G. Thus, it appears that, much like the computers, the Government is using the threat of delay in order to achieve its intended result.

19. Once one gets past the silly "this is just too hard for us" argument, one is left to wonder *why* the Government would want to allow the Defense the ability to post motions on its own, without any review or input from the Government. After all, the Government did say "The prosecution's ultimate concern is that the defense is picking and choosing what it thinks is appropriate for disclosure, which does not allow the United States to review the material." See Attachment B. The answer is obvious: the Government is waiting for a "gotcha" moment, where it can claim that the Defense has violated a protective order and caused grave and irreparable damage to the United States.

20. The Defense believes that the Government is setting the Defense up for another "spillage" incident, much like the one in March 2012.² Although this was never addressed on the record, the Defense believes that a spillage did *not* occur and that the Government misrepresented to the Court that an OCA had determined that a spillage occurred. See Attachment H ("I just got off the phone with CPT Fein. I called him to clarify whether there was a new claim of possible spillage. CPT Fein told me that there was not. His email simply referred to the claimed spillage from several weeks ago and possible issue he raised yesterday. Although not in his email, CPT

² To refresh the Court's memory, this is the incident where the Government submitted that the Defense had committed a spillage by inference. The Defense's motion did not contain any classified information. A separate attachment to the Defense's motion did not contain any classified information. However, the Government maintained that by reading these two separate documents together, one could infer classified information.

Fein represented to me that the OCA concluded the latest incident constituted spillage. I have asked CPT Fein to provide copies of any emails to the Defense and the Court that he sent to the OCA and received from the OCA regarding this issue. He did not indicate that he would provide the correspondence, or any portion thereof. ..."). The clear proof that a spillage did not occur is the fact that no remediation measures were ever taken after the alleged spillage. If indeed a spillage did occur, it was incumbent on the Government to take remediation measures. As such, the Defense submits that the Government misrepresented that a spillage had occurred in order to make the Defense look like it could not be trusted.

21. The risk that the Defense will post a motion that contains something that the Government deems objectionable is very real. This is evidenced by the Government complaining to the Court about the Defense's posting of a wholly innocuous description of what motions were to be argued at the upcoming motions argument. See Attachment B ("It is the government's understanding that the defense's posting of a summary of its motions violates the Court's interim order in that the government did not have the opportunity to object to this information prior to its posting. Although we have not had an opportunity to check with the different equity holders, there does not appear to be any information that we would otherwise protect in THIS posting. This action seems to be an attempt by the defense to bypass the procedures that the Court ordered."). So even though the Government did not have any actual concerns with "THIS" posting, it felt the need to tattle on the Defense.³

22. Moreover, the Government held the Defense to unreasonable standards with respect to the Court's protective order. The Government maintained that the Defense had to provide specific notice of its intent to publish individual motions; a blanket notice that the Defense would publish every motion that it filed was not enough. The following email exchange between the parties occurred on 30 May 2012 in respect of a motion that the Defense apparently did not give the Government specific notice of:

MAJ Fein: The defense never provided us notice that it intends to publish the Defense's response to the Government's motion for proposed LIOs.

Mr. Coombs: Read the Court's order. That is not required. You also have a 1 June deadline for the Defense replies.

MAJ Fein: Please see Appellate Exhibit LXVII, paragraph 1 under "ORDER:" for the notice provision.

Mr. Coombs: We will publish every substantive motion that that is on the case calendar, as we have in the past. I think it goes without saying but the Defense intends to publish its reply motions filed yesterday.

MAJ Fein: We will start processing this request. In the past, you have provided us notice through your email filings with the Court and we rely on those, pursuant

³ The Government had a similar "over the top" response when the Defense offered a redacted copy of the Grand Jury testimony into evidence. The Government complained that the Defense was waiving protected information around and that the information had to be under seal.

to the Court's order to know which filings will go. Please continue providing us the notice IAW the Court's order. What other filings would you like us to process?

Mr. Coombs: You are only behind on the Defense Response to the LIO motion. As stated, all replies will be filed publically [sic]. Under the Court's order, you have until 1 June to file a request for a protective order.

MAJ Fein: Thank you. As stated before, we are not behind any motion reviews. The defense is required to "notify the Government of each Defense Court filing or proposed filing intended for public release." Please continue to provide us notice of each filing or we will not process it. Without the affirmative notification, we cannot have certainty that the defense intends to make each one public, nor whether the defense intends to redact any motions. Please address any concerns with the Court's order with the military judge. We will start processing the Response to the Government's LIO Motion immediately and will get a response with the replies which were filed yesterday.

See Attachment I.

23. The Defense does not believe that the Court's order requires the Defense to specifically provide notice of each and every motion it intends to file publicly, given that it has already stated that it will file *every* motion publicly. The bigger point here is that the Government continually adopts unreasonable litigation positions – and the Defense expects to see this behavior continue if the Defense permitted to file motions publicly without the Government's input.

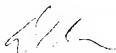
24. Aside from the Court's Protective Order, the Defense has had no guidance from the Government on what may or may not be objectionable. To date, the Defense has over-redacted its filings simply because it does not feel like getting into an irrational debate with the Government over the redactions. However, the Defense still does not know what information (aside from information subject to a protective order) the Government might suddenly deem problematic. Consequently, the Defense does not want to risk the near-certain fate that will result if the Defense files a motion without the Government's blessing: the infamous "gotcha" moment. This is of particular concern since the Protective Order still does not specify the circumstances under which the Government might decide to report Defense counsel to their state bar association.

25. The Government's final request is that the Court "order the defense to redact an individual's job title or position, if that individual is not a party to the trial and only one individual holds that job title or position." The Defense does not object to this. However, with so much in the public domain already and the individuals being referred to by title and name in open court, the request appears to be pointless. Moreover, the proffered reason for the redaction – "to protect the safety of potential witnesses" – seems far-fetched to say the least. Nonetheless, the Defense will endeavor to comply with the Government's request.

CONCLUSION

26. Since the Court's Protective Order has been in place, there have not been any subsequent claims of spillage or violations of the Court's Protective Order by the Government. The motions practice is almost completed. The Government would seek to fix what is not broken at this point. For the reasons stated above, the Defense respectfully requests that this Court deny the Government's motion.

Respectfully submitted,



DAVID EDWARD COOMBS
Civilian Defense Counsel

ATTACHMENT A

David Coombs

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA <Ashden.Fein@jfhqncr.northcom.mil>
Sent: Friday, March 23, 2012 5:33 PM
To: Lind, Denise R COL USARMY (US)
Cc: David Coombs; Matthew kemkes; Bouchard, Paul R CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA; ashden.fein@us.army.mil; Prather, Jay R CIV (US); Williams, Patricia CIV JFHQ-NCR/MDW SJA
Subject: Defense's Release of Court Filings

Ma'am,

The United States opposes the defense's request to freely publish all motions, responses, and replies on the Internet. The defense's request would act to publicize information provided to the defense in discovery, the public disclosure of which may require outside agency approval and the substance of which may cause irreparable prejudice to the United States. Much of the information in this case was disclosed under various protective orders which remain in effect, including grand jury subpoena information, Secretary of the Army 15-6 investigation information, and law enforcement sensitive information. This protected information was provided to the defense for discovery and under the specific condition not to publish or release it outside of the specific individuals who were allowed access to the information.

The defense purports that it wants to publish this information online to keep the public informed of the proceeding. The public, however, is already well informed of the proceedings. The public was present at the Article 32 hearing, the arraignment, and the first motions hearing, and will continue to be present at all open portions of the motions hearings and the trial. The command provided the theater next door for overflow area so that the public can freely watch the proceedings and the media operations center for the media. Additionally, other than the electronic filing process, the military justice system is more open than the federal system from the Article 32 proceedings through the end of the trial.

The United States does not intend to publish its pleadings online. If the defense remains intent on publishing all pleadings and their enclosures online, the United States requests the opportunity to file a motion for a protective order or multiple protective orders under RCM 701(g)(2) and 806(d) for the Court to regulate the defense's use of information gained through discovery. Additionally the United States requests the Court allow the prosecution thirty days to receive input from all the different federal entities on what information they provided for discovery which they did not intend to be made publically available. The sole purpose of discovery is to prepare for trial. Motions are filed to shape legal issues and belong to the Court. Most motions, e.g., motions to suppress or exclude evidence or testimony, are not appropriate for publication. Freely publicizing all pleadings, at this stage of the proceedings, may undermine the effectiveness of the publicity order and will circumvent those measures adopted to regulate what is available to the public and significantly jeopardize many interests of the United States, to include, protecting classified information (in the case of a spillage), preserving the confidentiality of law enforcement information, preventing potential witnesses from receiving information outside the scope of their projected testimony, protecting testifying witnesses, protecting trial participant safety, protecting the personal information of potential panel members, preventing disclosure of government information that threatens national security and is unclassified, and the deliberative processes of the United States Government. Furthermore, the United States believes that the defense's intended course of action would result in a substantial likelihood of materially prejudicing the proceeding, in violation of, inter alia, RCM 806(d) and Army Regulation 27-26, specifically Rule 3.6.

v/r
MAJ Fein

ATTACHMENT B

David Coombs

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA <Ashden.Fein@jfhqncr.northcom.mil>
Sent: Monday, April 02, 2012 10:08 AM
To: Lind, Denise R COL USARMY (US)
Cc: David Coombs; Kemkes, Matthew J MAJ USARMY (US); Bouchard, Paul R CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA; Prather, Jay R CIV (US); Williams, Patricia CIV JFHQ-NCR/MDW SJA
Subject: Interim Order Clarification
Attachments: Blog Printout.pdf

Ma'am,

Good morning. Could you please clarify a portion of your interim order (Government Request for Leave to File Protective Order(s))? It was the government's understanding that we would have an opportunity to redact and/or object to the defense posting the Defense filings or proposed filings before the defense posts the information to the internet. Although the defense has not posted its actual filings or proposed filings, the defense has posted information that speaks directly to the substance of its proposed filings:

"...if the redacted motions are not available, the following will provide a general understanding of what Defense motions are being addressed on April 24th through 26th...." The entire posting is attached for your reference.

It is the government's understanding that the defense's posting of a summary of its motions violates the Court's interim order in that the government did not have the opportunity to object to this information prior to its posting. Although we have not had an opportunity to check with the different equity holders, there does not appear to be any information that we would otherwise protect in THIS posting. This action seems to be an attempt by the defense to bypass the procedures that the Court ordered. The prosecution's ultimate concern is that the defense is picking and choosing what it thinks is appropriate for disclosure, which does not allow the United States to review the material. It is the government's duty to protect individuals and information, ensure the integrity of the process and a fair trial, which includes protecting overly prejudicial information, as well as unclassified but protected and classified information.

Could you please provide clarification on what the defense is authorized to post and whether the government will have the opportunity to review the information prior to posting?

Thank you.

v/r
MAJ Fein

ATTACHMENT C

David Coombs

From: Lind, Denise R COL USARMY (US) <denise.r.lind.mil@mail.mil>
Sent: Monday, April 02, 2012 1:50 PM
To: Fein, Ashden MAJ USARMY (US)
Cc: David Coombs; Kemkes, Matthew J MAJ USARMY (US); Bouchard, Paul R CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M CPT USARMY (US); Whyte, Jeffrey H CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US); Prather, Jay R CIV (US); Williams, Patricia A CIV (US)
Subject: RE: Interim Order Clarification
Signed By: denise.lind@us.army.mil

Counsel,

The intent of the interim order was to ensure no information was published outside of court that included information from discovery via protective order, information subject to privilege under MRE 505 and 506, and PII to protect witness/participant privacy and safety. The interim order was not intended to prevent the defense from publishing their legal theory for upcoming motions.

If the government identifies particular publications by the defense the government believes warrants a more broad protective order, the government may raise the issue at the next article 39(a) session, or, if necessary, request a telephonic RCM 802 conference with the Court.

D

Denise R. Lind
COL, JA
Chief Judge, 1st Judicial Circuit

-----Original Message-----

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA
[\[mailto:Ashden.Fein@jfhqncr.northcom.mil\]](mailto:Ashden.Fein@jfhqncr.northcom.mil)
Sent: Monday, April 02, 2012 10:08 AM
To: Lind, Denise R COL USARMY (US)
Cc: David Coombs; Kemkes, Matthew J MAJ USARMY (US); Bouchard, Paul R CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M CPT USARMY (US); Whyte, Jeffrey H CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US); Prather, Jay R CIV (US); Williams, Patricia A CIV (US)
Subject: Interim Order Clarification

Ma'am,

Good morning. Could you please clarify a portion of your interim order

ATTACHMENT D

-----Original Message-----

From: David Coombs [<mailto:coombs@armycourtartialdefense.com>]

Sent: Thursday, March 29, 2012 7:09 PM

To: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA

Cc: 'Prather, Jay R CIV (US)'; 'Kemkes, Matthew J MAJ USARMY (US)'; 'Bouchard, Paul R CPT USARMY (US)'; 'Joshua Tooman'; 'Santiago, Melissa S CW2 USARMY (US)'; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA

Subject: Redactions

Ashden,

I am in the process of conducting my redactions. I would like to get the Government's position on whether you would have any objection to the following:

- a) Quoting statements by Government counsel during arguments;
- b) Quoting from Government Pleadings;
- c) Quoting emails from the Government to the Court and/or the Defense; and
- d) Quoting Court Rulings.

Best,
David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906
Toll Free: 1-800-588-4156
Local: (508) 689-4616
Fax: (508) 689-9282
coombs@armycourtartialdefense.com
www.armycourtartialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

ATTACHMENT E

From: "Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA"

<Ashden.Fein@jfhqncr.northcom.mil>

(Add as Preferred
Sender)

Date: Thu, Mar 29, 2012 8:38 pm

To: "David Coombs" <coombs@armycourtmarialdefense.com>

Cc: "Kemkes, Matthew J MAJ USARMY (US)" <matthew.j.kemkes.mil@mail.mil>, "Bouchard, Paul R CPT USARMY (US)" <paul.r.bouchard.mil@mail.mil>, "Joshua Tooman"

<joshua.j.tooman.mil@mail.mil>, "Santiago, Melissa S CW2 USARMY (US)"

<melissa.s.santiago.mil@mail.mil>, "Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA"

<JoDean.Morrow@jfhqncr.northcom.mil>, "Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA"

<Angel.Overgaard@jfhqncr.northcom.mil>, "Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA"

<Jeffrey.Whyte@jfhqncr.northcom.mil>, "Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA"

<Arthur.Ford@jfhqncr.northcom.mil>

David,

The government has no objection to a and d below because those are matters of public record, so long as they are accurate. Depending on what is written in b and c, the government might have an objection.

v/r

Ashden

ATTACHMENT F

-----Original Message-----

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA [<mailto:Ashden.Fein@jfhqncr.northcom.mil>]

Sent: Thursday, April 05, 2012 2:25 PM

To: David Coombs; Lind, Denise R COL MIL USA OTJAG

Cc: Kemkes, Matthew J MAJ USARMY (US); Bouchard, Paul R CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA; Prather, Jay R CIV (US); Williams, Patricia CIV JFHQ-NCR/MDW SJA

Subject: RE: Redactions

Mr. Coombs,

We are still working on reviewing these documents. Right away we noticed that none of the information is actually redacted, but rather have black highlights, so anyone can copy and paste the information from behind the black boxes. Additionally individual email addresses within the document can still be "clicked" to send an email to the redacted individuals.

In order to make this process more efficient, the United States recommends that you submit the documents to us with see-through redaction boxes (or colored highlights) so all parties can read the information behind the redaction and the documents can be more easily reviewed by the prosecution and any relevant federal entity. After our review, we will return the document with proposed redaction boxes (or colored highlights). For this first round, we will recreate your redactions on a clean document with redaction boxes, so the process can continue moving forward quickly and efficiently.

Thank you.

v/r

MAJ Fein

ATTACHMENT G

From: "Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA"

(Add as Preferred
Sender)

<Ashden.Fein@jfhqncr.northcom.mil>

Date: Mon, Apr 16, 2012 5:31 pm

To: "David Coombs" <coombs@armycourtmarshaldefense.com>

Cc: <joshua.i.tooman.mil@mail.mil>, <melissa.s.santiago.mil@mail.mil>, "Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA" <JoDean.Morrow@jfhqncr.northcom.mil>, "Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA" <Angel.Overgaard@jfhqncr.northcom.mil>, "Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA" <Jeffrey.Whyte@jfhqncr.northcom.mil>, "VonElten, Alexander S. 1LT USA JFHQ-NCR/MDW SJA" <Alexander.VonElten@jfhqncr.northcom.mil>, "Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA" <Arthur.Ford@jfhqncr.northcom.mil>

David,

As for the forensic drives, CID will continue examining the drives as per the Court's order and we will provide the results by 20 April 2012. However, in an effort to save time and resources for all parties involved (defense, government computer experts, government classification experts), we can produce the forensic images of the drives, as per the defense's original request. The defense will be able to conduct any analysis/procedure it wishes with complete copies of the drives.

We can wait until after 20 April 2012, however it will take more time after that to get those drives fully reviewed for security classification purposes, than merely the filenames. If the defense ultimately wants the forensic images and access to the files (as per the original motion and the renewed motion) sooner than later, the United States recommends the defense support this way forward, so we can divert CID resources from continuing to search for these programs and having to dedicate security experts to the review of the lists, and just have all of them focus on the actual files. We are confident we will be able to have them reviewed and approved, absent some unusual issue, by 18 May 2012.

Following this email, I will send you responses to your questions from Friday. My previous email was intended to simply explain that I will provide you answers by COB today, for your questions you asked on Friday.

v/r
Ashden

ATTACHMENT H

From: <coombs@armycourtartialdefense.com>(Add as Preferred Sender)
Date: Wed, Mar 14, 2012 9:08 pm
To: "Fein, Ashden CPT USA JFHQ-NCR/MDW SJA" <Ashden.Fein@fhqncr.northcom.mil>, "Lind, Denise R COL MIL USA OTJAG" <denise.r.lind.mil@mail.mil>
Cc: "Matthew kemkes" <matthew.kemkes@us.army.mil>, "Bouchard, Paul R CPT USARMY (US)" <paul.r.bouchard.mil@mail.mil>, "Jefferson, DaShawn MSG MIL USA OTJAG" <dashawn.jefferson.mil@mail.mil>, "Joshua Tooman" <joshua.j.tooman.mil@mail.mil>, "Melissa Santiago" <melissa.s.santiago@us.army.mil>, "Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA" <JoDean.Morrow@fhqncr.northcom.mil>, "Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA" <Angel.Overgaard@fhqncr.northcom.mil>, "Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA" <Jeffrey.Whyte@fhqncr.northcom.mil>, "Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA" <Arthur.Ford@fhqncr.northcom.mil>

Ma'am,

I just got off the phone with CPT Fein. I called him to clarify whether there was a new claim of possible spillage. CPT Fein told me that there was not. His email simply referred to the claimed spillage from several weeks ago and possible issue he raised yesterday.

Although not in his email, CPT Fein represented to me that the OCA concluded the latest incident constituted spillage. I have asked CPT Fein to be provide copies of any emails to the Defense and the Court that he sent to the OCA and received from the OCA regarding this issue. He did not indicate that he would provide the correspondence, or any portion thereof. He advised that he would take the issue up with you tomorrow.

Best,
David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906
Toll Free: 1-800-588-4156
Local: (508) 689-4616
Fax: (508) 689-9282
coombs@armycourtartialdefense.com
www.armycourtartialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

ATTACHMENT I

David Coombs

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA <Ashden.Fein@jfhqncr.northcom.mil>
Sent: Wednesday, May 30, 2012 11:05 AM
To: David Coombs; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA
Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US)
Subject: RE: Motion for Protective Order on Defense Response Motion

David,

We will have an answer by 1 Jun. Thank you.

v/r
Ashden

-----Original Message-----

From: David Coombs [mailto:coombs@armycourt martialdefense.com]
Sent: Wednesday, May 30, 2012 10:41 AM
To: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA
Cc: Hurley, Thomas F MAJ USARMY (US); 'Tooman, Joshua J CPT USARMY (US)'
Subject: RE: Motion for Protective Order on Defense Response Motion

Ashden,

The Government has until 1 June to file any requested protective order on the replies. If you need until 1 June for the Defense Response to the Government's LIO motion, that is not a problem.

Best,
David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906
Toll Free: 1-800-588-4156
Local: (508) 689-4616
Fax: (508) 689-9282
coombs@armycourt martialdefense.com
www.armycourt martialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

-----Original Message-----

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA [mailto:Ashden.Fein@jfhqncr.northcom.mil]

Sent: Wednesday, May 30, 2012 10:31 AM

To: David Coombs; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA

Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US)

Subject: RE: Motion for Protective Order on Defense Response Motion

David,

Thank you. As stated before, we are not behind any motion reviews. The defense is required to "notify the Government of each Defense Court filing or proposed filing intended for public release." Please continue to provide us notice of each filing or we will not process it. Without the affirmative notification, we cannot have certainty that the defense intends to make each one public, nor whether the defense intends to redact any motions. Please address any concerns with the Court's order with the military judge.

We will start processing the Response to the Government's LIO Motion immediately and will get a response with the replies which were filed yesterday.

v/r

Ashden

-----Original Message-----

From: David Coombs [mailto:coombs@armycourt martialdefense.com]

Sent: Wednesday, May 30, 2012 10:11 AM

To: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA

Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US)

Subject: RE: Motion for Protective Order on Defense Response Motion

Ashden,

You are only behind on the Defense Response to the LIO motion. As stated, all replies will be filed publically. Under the Court's order, you have until 1 June to file a request for a protective order.

Best,

David

David E. Coombs, Esq.

Law Office of David E. Coombs

11 South Angell Street, #317

Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282

coombs@armycourt martialdefense.com

www.armycourt martialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

-----Original Message-----

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA (mailto:Ashden.Fein@jfhqncr.northcom.mil)

Sent: Wednesday, May 30, 2012 10:08 AM

To: David Coombs; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA

Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US)

Subject: RE: Motion for Protective Order on Defense Response Motion

David,

We will start processing this request. In the past, you have provided us notice through your email filings with the Court and we rely on those, pursuant to the Court's order to know which filings will go. Please continue providing us the notice IAW the Court's order. What other filings would you like us to process?

v/r

Ashden

-----Original Message-----

From: David Coombs (mailto:coombs@armycourt martialdefense.com)

Sent: Wednesday, May 30, 2012 10:06 AM

To: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA

Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US)

Subject: RE: Motion for Protective Order on Defense Response Motion

Ashden,

We will publish every substantive motion that that is on the case calendar, as we have in the past. I think it goes without saying but the Defense intends to publish its reply motions filed yesterday.

Best,

David

David E. Coombs, Esq.

Law Office of David E. Coombs

11 South Angell Street, #317

Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282

coombs@armycourt martialdefense.com

www.armycourt martialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

-----Original Message-----

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA [mailto:Ashden.Fein@jfhqncr.northcom.mil]
Sent: Wednesday, May 30, 2012 10:02 AM
To: David Coombs; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA
Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US)
Subject: RE: Motion for Protective Order on Defense Response Motion

David,

Please see Appellate Exhibit LXVII, paragraph 1 under "ORDER:" for the notice provision.

v/r
Ashden

-----Original Message-----

From: David Coombs [mailto:coombs@armycourt martialdefense.com]
Sent: Wednesday, May 30, 2012 10:00 AM
To: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA
Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US)
Subject: RE: Motion for Protective Order on Defense Response Motion

Ashden,

Read the Court's order. That is not required. You also have a 1 June deadline for the Defense replies.

Best,
David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906
Toll Free: 1-800-588-4156
Local: (508) 689-4616
Fax: (508) 689-9282
coombs@armycourt martialdefense.com
www.armycourt martialdefense.com

Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.

-----Original Message-----

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA [mailto:Ashden.Fein@jfhqncr.northcom.mil]
Sent: Wednesday, May 30, 2012 9:58 AM
To: David Coombs; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA
Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US)
Subject: RE: Motion for Protective Order on Defense Response Motion

David,

The defense never provided us notice that it intends to publish the Defense's response to the Government's motion for proposed LIOs.

V/r
Ashden

-----Original Message-----

From: David Coombs [mailto:coombs@armycourt martialdefense.com]
Sent: Wednesday, May 30, 2012 9:48 AM
To: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA
Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US)
Subject: Motion for Protective Order on Defense Response Motion

Ashden,

The Government did not file a motion for a protective order concerning the Defense's Response LIO Motion by the filing date for replies as required by the Court's order. Does this mean that you have no objection or requested redactions?

Best,

David

David E. Coombs, Esq.
Law Office of David E. Coombs
11 South Angell Street, #317
Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282

coombs@armycourtartialdefense.com
<mailto:coombs@armycourtartialdefense.com>

www.armycourtartialdefense.com <<http://www.armycourtartialdefense.com/>>

*****Confidentiality Notice:** This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.***

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army,)

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

**DEFENSE RESPONSE TO
GOVERNMENT MOTION FOR
ADMISSION OF EVIDENCE
UNDER M.R.E. 803(6)**

DATED: 6 July 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, moves this court to deny the Government's motion in part.¹

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Government has the burden of persuasion. R.C.M. 905(c)(2). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010).

4. The original charges were preferred on 5 July 2010. Those charges were dismissed by the convening authority on 18 March 2011. The current charges were preferred on 1 March 2011. On 16 December through 22 December 2011, these charges were investigated by an Article 32 Investigating Officer. The charges were referred on 3 February 2012.

¹ The Defense does not oppose the admissibility of Enclosures 1, 2, 3, 4, 5, 6, 7, 14 and 15 to the Government's motion for Preliminary Ruling on Admissibility of Evidence dated 22 June 2012. The Defense does oppose admission of Enclosures 8, 9, 10, 11, 12 and 13 of the same Government motion.

WITNESSES/EVIDENCE

5. The Defense does not request any witnesses be produced for this motion.

LEGAL AUTHORITY AND ARGUMENT

6. The Defense objects to the admission of Enclosures 8, 9, 10, 11, 12 and 13 to the Government's motion for Preliminary Ruling on Admissibility of Evidence dated 22 June 2012 because they are testimonial hearsay falling outside the scope of M.R.Es 803(6) and 902(11).

7. M.R.E. 803(6) establishes an exception to the general rule against hearsay where records are kept in the course of "regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or be certification that complies with M.R.E. 902(11)."

8. Despite this exception to the prohibition against hearsay, a business record must also satisfy the 6th Amendment's Confrontation Clause. The Court in *Crawford v. Washington* established that where testimonial hearsay is at issue, the Confrontation Clause is only satisfied if the accused is afforded an opportunity for cross-examination. 541 U.S. 36, 59 (2004). The *Crawford* Court defined testimonial hearsay further as "statements that were made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial." *Id.* at 51.

9. C.A.A.F.'s ruling in *U.S. v. Rankin*, 64 M.J. 348 (2007), is instructive on what amounts to testimonial hearsay in the military context. There, the court established a three-part test for identifying testimonial hearsay:

(1) was the statement at issue elicited by or made in response to law enforcement or prosecutorial inquiry; (2) did the statement involve more than a routine and objective cataloging of unambiguous factual matters; and (3) was the primary purpose for making, or eliciting, the statement the production of evidence with an eye toward trial.

Id. at 352.

10. The C.A.A.F. in *U.S. v. Harcrow*, applied the Rankin factors when considering whether laboratory reports created upon request by the county sheriff were testimonial. 66 M.J. 154 (2008). In considering the Confrontation Clause issue, the court noted, "[h]ere the laboratory tests were specifically requested by law enforcement and the information relayed on the laboratory reports pertained to items seized during the arrest of an identified 'suspect.'" *Id.* at 159. The court further held, "lab results or other types of routine records may become testimonial where a defendant is already under investigation, and where the testing is initiated by the prosecution to discover incriminating evidence." *Id.* (quoting *U.S. v. Magyari*, 63 M.J. 123 (2006)).

11. Similarly, the Coast Guard Court of Criminal Appeals applied the *Rankin* Factors in determining whether statements in a cover memorandum were testimonial. *U.S. v. Byrne*, 70 M.J. 611 (2011). In *Byrne*, the court found the Confrontation Clause had been violated when a "Laboratory Document Packet" regarding an alleged positive urinalysis was admitted over defense objection. In weighing the *Rankin* factors the Court noted, "we find the statements in the cover memorandum were made in response to a request for a litigation packet, which clearly indicates that a court-martial is being contemplated, and, thus, the memorandum was prepared in response to a prosecutorial inquiry." *Id.* at 614.

12. In the case at hand, the Government seeks to introduce several enclosures that are testimonial in nature. Specifically, enclosures 8, 9, and 10 to the Government's motion dated 22 June fall outside the scope of 803(6) and 902(11) because they were made in preparation for trial. Because they were made in preparation for trial, they are testimonial in nature and, pursuant to *Rankin* and the 6th Amendment, should not be admitted at this time.

a. Enclosure 8 is a pair of screen shots allegedly showing the dates PFC Manning completed IA training and his user profile for the Army Training and Certification Tracking System. These documents are not admissible because they were produced in preparation for trial. Enclosure 11, an Agent Investigative Report (AIR) written by SA Troy M. Bettencourt on 21 January 2011, clearly demonstrates that Enclosure 8 was produced at the behest of law enforcement. It is safe to assume that Mr. John Sciandra did not email SA Bettencourt out of the blue with screenshots related to PFC Manning. Rather, he must have been replying to a Government inquiry. Moreover, the date of the AIR, 21 January 2011, falls after prefferal of charges and serves as a crystal clear indication that the records were produced with an eye towards litigation. When considering these facts in light of *Rankin* and its progeny, it is clear that Enclosure 8 does not qualify for admission under 803(6) and 902(11).

b. Enclosure 9 is a screenshot of PFC Manning's U.S. Army Information Assurance Virtual Training profile. Like Enclosure 8, this document was clearly produced at the behest of the Government with an eye towards litigation, as it is also referenced in the AIR by SA Bettencourt. Because such facts weight both the first and third *Rankin* factors in PFC Manning's favor, this document should not be admitted under 803(6) and 902(11). To do so would violate PFC Manning's right to confrontation under the 6th Amendment.

c. As mentioned, Enclosure 10 is an AIR from SA Bettencourt. This document was clearly prepared in preparation for litigation and, thus, qualifies as testimonial under the *Rankin* factors. Moreover, it lacks the requisite attestation under M.R.E. 803(6) and 902(11). As such, the Government's motion should be denied.

13. Enclosures 11 also falls outside the scope of 803(6) and 902(11) because it, too, was made in preparation for trial. Enclosure 11 is a Joint Asset Movement Management System (JAMMS) report allegedly pertaining to PFC Manning. The date on both the report and attestation certificate is 15 February 2012, which is after both prefferal and referral of the charges against


PFC Manning. It is unlikely that Ms. Mary Amatu, the signatory of the attestation certificate, woke up on the morning of 15 February 2012, decided to pull PFC Manning's records and then signed a certificate attesting that the records meet the requirements of the Military Rules of Evidence. Rather, it is more likely that Ms. Amatu created the record at the behest of the Trial Counsel in this case. Like the reports discussed in *Harcrow*, Enclosure 11 is a report that was created upon a specific request by the Government, relates to an individual who is facing a court-martial and is offered to prove an element of one of the alleged crimes. *Harcrow* at 159; see also *Magyari*. Because Enclosure 11 was created upon request by the Government, relates to PFC Manning and is offered to prove an element of one or more of PFC Manning's alleged crimes, the document is testimonial in nature. As testimonial hearsay, Enclosure 11 should not be admitted at this time, lest PFC Manning's right to confrontation be violated.

14. Finally, Enclosures 12 and 13 should also not be admitted because they do not comport with the attestation requirement of MRE 803(6). Enclosure 12 is an AIR scribed by SA Hyung Kim, while Enclosure 13 is a one page synopsis of the Distributed Common Ground System-Army (DCGS-A) system evidently prepared by General Dynamics. Neither enclosure includes an attestation certificate as contemplated by 902(11), nor does the Government's motion give any indication that a witness will be called to attest that the "business records" are maintained in conformity with MRE 803(6). Moreover, Enclosure 12, SA Kim's AIR dated 31 August 2010, was clearly made as part of the investigation into PFC Manning's alleged misconduct and with an eye towards a trial as it is dated post-preferred. It is, thus, testimonial and the Confrontation Clause demands examination of SA Kim if the Government wishes to admit information contained within her AIR.

CONCLUSION

15. Based on the above, the Defense requests that the Court deny, in part, the Government's motion to pre-admit evidence under R.C.M. 902(11).

Respectfully submitted,



JOSHUA J. TOOMAN
CPT, JA

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES)

v.)

MANNING, Bradley E., PFC)

U.S. Army, [REDACTED])

Headquarters and Headquarters Company, U.S.)

Army Garrison, Joint Base Myer-Henderson Hall,)

Fort Myer, VA 22211)

**DEFENSE NOTICE UNDER
MILITARY RULE OF EVIDENCE
505(h)(3): CHARGED
DOCUMENTS**

DATED: 6 July 2012

1. The Government previously provided notice to the Defense of the following charged documents:

- a) Batch #1 (00376954 – 00377572);
- b) Batch #2 (00377626 – 00377675); and
- c) Batch #3 (00377845 – 00378140).

2) Pursuant to Military Rule of Evidence 505(h)(3), PFC Manning, by and through counsel, provides notice to the Government that the Defense intends to present, either through cross-examination of a Government's witnesses or during the Defense's presentation, the following listed evidence from the charged documents:

- a) CIDNE Afghanistan Significant Activity Reports (SIGACTs). The Defense intends to discuss the 43 individual SIGACT reports that are the subject of Specification 7 of Charge II either on cross examination or through the testimony of a Defense witness. The 43 SIGACT reports are labeled as Bates Number 00377846 through 00377911. Specifically, the Defense intends to discuss the content of the 43 SIGACTs, and the OCA's classification determination regarding the possible impact on national security from having this information released publicly. Of the 43 SIGACTs that the Defense intends to discuss, the following 5 were listed in the charged documents, but were not part of the OCA's classification review: 00377847-48; 00377857-58; 00377859; 00377872-73; and 00377884-85. The Defense also intends to discuss, in general, the Afghanistan SIGACT reports that are the subject of Specification 6 of Charge II. The CIDNE Afghanistan SIGACTs consisted of 91,731 documents covering a period from 1 January 2004 to 31 December 2009.
- b) CIDNE Iraq SIGACTs. The Defense intends to discuss the 61 individual SIGACT reports that are the subject of Specification 5 of Charge II either on cross examination or through the testimony of a Defense witness. The 61 SIGACT reports are labeled as Bates Number 00377912 through 00378027. Specifically, the Defense intends to discuss the content of the 61 SIGACTs, and the OCA's classification determination regarding the

possible impact on national security from having this information released publicly. Of the 61 SIGACTs that the Defense intends to discuss, the following 8 were listed in the charged documents, but were not part of the OCA's classification review: 00377920; 00377939; 00377950-51; 00377959; 0037981-82; 00377987; 00378014-15; and 00378027. The Defense also intends to discuss, in general, the Iraq SIGACT reports that are the subject of Specification 4 of Charge II. The CIDNE Iraq SIGACTs consist of 391,832 documents covering a period from 1 January 2004 to 31 December 2009;

- c) Other Briefings, Memorandums, Documents, a Video and accompanying 15-6 Investigation Report. The items referenced are the subject of Specifications 10 and 11 of Charge II. This information contains FRAGO orders, several memorandums, a battle drill matrix for civilian casualties, rules of engagement memorandums, PowerPoint presentations, and a four minute surveillance video of individuals leaving a building and then walking along a path. The four minute surveillance video does not depict the airstrike that took place on 4 May 2009 (commonly referred to as the Granai airstrike) which resulted anywhere between 80 to 140 civilians being killed. However, the video was apparently made on the same day as the Granai airstrike. The Defense intends to discuss the video and each of the following items listed within the charged documents and/or within the OCA's classification review at Bates number 00376901-02 either on cross examination or through the testimony of a Defense witness:
- i. Brief to GEN P Finding and Recs: 00377425-428;
 - ii. Farah Brief FINAL v2 22 May 09: 00377429-53;
 - iii. Farah Brief FINAL v8 24 May 09: 00377454-79;
 - iv. Tab A Appendix 10 (USFOR-A FRAGO 08-003 – CIVCAS Procedures) Sep 08: 00377480-92;
 - v. CENTCOM Positive Identification Policy: 00377493-495 (*apparently not part of OCA review);
 - vi. Tab D Appendix 7 (8141 Initial TIC Slide) 4 May 09: 00377496-98;
 - vii. Final – IO'S Report (OS 20002 JUN 09)(Signed)(minimized)(3): 00378029-65;
 - viii. Tab A Appendix 1 (CISOTF FRAGO 02 – Operational Guidance) 29 Jan 09: 00378066-070;
 - ix. Tab A Appendix 2 (FRAGO 429-2008 COMISAF TAC DIR) 08 Dec 08: 00378071-78;
 - x. Tab A Appendix 5 (USCENTCOM Tactical Directive – OEF AFG) 12 Sep 08: 00378079-81;
 - xi. Strategic intel brief, 10 May 2009 "Farah INS Probably Deliberately Instigated": 00378082-83;
 - xii. Tab A Appendix 12 (USCENTCOM consolidated Serial One Rules of Engagement for Operation Enduring Freedom MOD 002) 15 Dec 06: 00377627-37;
 - xiii. ORF Support Farah ETT (8141) PowerPoint document May 2009: 00377672-73;
 - xiv. Tab D Appendix 6 (8213 QRF CONOP) 4 May 09: 00377674-75; and
 - xv. BE22 Pax Zip Video: 00378028.

Some of this information also appears to be the subject of Rear Admiral Kevin Donegan's classification review at Bates number 00376872-73. Specifically, the Defense intends to discuss the content of the above listed items and the OCA's classification review and determinations regarding the possible impact on national security from having this information released publicly.

- d) Reykjavik-13 Diplomatic Cable at Bates Number 00377392-94. This diplomatic cable was from the embassy in Reykjavik detailing the financial difficulties of a privately owned Icelandic bank called Landsbanki, which offered online savings accounts under the "Icesave" brand. The bank was placed into receivership by the Icelandic Financial Supervisory Authority on 7 October 2008. The Defense intends to discuss the diplomatic cable that is the subject of Specification 14 of Charge II either on cross examination or through the testimony of a Defense witness. Specifically, the Defense intends to discuss the content of the Reykjavik-13 cable and the OCA's classification determination regarding the possible impact on national security from having this information released publicly.
- e) Diplomatic Cable Database. The Defense intends to discuss each of the 125 diplomatic cables that is the subject of Specification 13 of Charge II either on cross examination or through the testimony of a Defense witness. The 125 diplomatic cables are labeled as Bates Number 00376954 through 00377424; 00377499 through 00377572; and 00377638 through 00377675. Specifically, the Defense intends to discuss the content of the 125 diplomatic cables and the OCA's classification determination regarding the possible impact on national security from having this information released publicly. Of the 125 diplomatic cables the Defense intends to discuss, the following 9 were listed in the charged documents, but were not part of the OCA's classification review: 00376960-63; 00377031-32; 00377045-48; 00377099-103; 00377137-40; 00377186-87; 00377366-69; 00377526-29; and 00377654-59. Additionally, the following cable was part of the OCA's classification review, but was not part of the charged documents: 07BAGHDAD42. The Defense also intends to discuss the diplomatic cables in general that are the subject of Specification 12 of Charge II. The contents of these cables describe international affairs from 300 embassies dating from 1966 to 2010. This database contains 251,287 documents. Over 130,000 of the documents are unclassified, some 100,000 are labeled "confidential", about 15,000 documents are classified as "secret", and none are classified as "top secret".
- f) Apache Helicopter Video Bates Number 00377845. Although this video is not classified, the Defense provides notice that it intends to discuss the Apache helicopter video that is the subject of Specification 2 of Charge II either on cross examination or through the testimony of a Defense. Specifically, the Defense intends to discuss CPT James Kolky's classification review and the classification review at 00419522. The Defense intends to offer evidence from these reviews discussing the lack of impact on national security from having this information released publicly. The charged video is a thirty-nine minute Apache cockpit gun-sight video depicting a series of air-to-ground attacks conducted by a team of two U.S. Army AH-64 Apache helicopters in Al-Amin al-Thaniyah, in the district of New Baghdad in Baghdad. The attacks took place on 12 July 2007. In the

first strike, 30mm cannon fire was directed at a group of nine men; two were war correspondents for Reuters – Saeed Chmagh and Namir Noor-Elden. Eight men were killed, including Noor-Eldeen. Chmagh was wounded. In the second airstrike, 30mm cannon fire was directed at Chmagh and two other unarmed men and their unmarked van as they were attempting to help Chmagh into the van. Two children inside the van were wounded, three more men were killed, including Chmagh. In a third airstrike, an Apache helicopter team fired three AGM-114 Hellfire missiles to destroy a building after they had observed men enter the building.

- g) U.S. Army's Counterintelligence Assessment Bates Number 00378091-122. The Defense intends to discuss the document that is the subject of Specification 15 of Charge II either on cross examination or through the testimony of a Defense witness. Specifically, the Defense intends to discuss the content of the document and the OCA's classification determination regarding the lack of impact on national security from having this information released publicly. The Defense also intends to discuss the review of the charged document in 00377733-35. The Charged document is a thirty-two page document prepared by the Cyber Counterintelligence Assessments Branch of the Army's Counterintelligence Center along with the National Ground Intelligence Center to assess the possible threat posed to the U.S. Army by disclosures to WikiLeaks.
- h) The Detainee Assessment Briefs Bates Number 00378123-40. The Defense intends to discuss each of the 22 pages (18 Bates Numbered pages) that is the subject of Specification 9 of Charge II either on cross examination or through the testimony of a Defense witness. Specifically, the Defense intends to discuss the content of the documents and the OCA's classification determination regarding the impact on national security from having this information released publicly. The Defense also intends to discuss, in general, the detainee assessment brief database that are the subject of Specification 8 of Charge II. This database consists of 779 multi-page memorandums. Each memorandum contains information about a detainee to include their background; how they were captured; whether they are regarded as low, medium, or high risk; and whether they should be released or not.
- i) Government Intelligence Agency Memorandums Bates Number 00378084-90. The Defense intends to discuss each of the 7 pages that is the subject of Specification 3 of Charge II either on cross examination or through the testimony of a Defense witness. The Defense also intends to discuss the review of the charged document in 00447841-45. Specifically, the Defense intends to discuss the content of the documents and the OCA's classification determination regarding the impact on national security from having this information released publicly.
- j) Chat Logs (not within charged documents). The Defense intends to discuss the content of the computer chat session allegedly had between Mr. Adrian Lamo and PFC Manning either on cross examination or through the testimony of a Defense witness. The chat log has no classification markings, but according to one OCA, the chat conversation may contain classified information. The chat logs were not within the charged documents, but do appear to be part of the classification review by Vice Admiral Robert Harward. The

Defense intends to discuss the content of the chat conversation and any OCA's classification determination regarding the impact on national security from having this information released publicly.

3. Nothing contained in this notice should be construed in any manner as a concession by PFC Manning or his Defense that the listed items are appropriately classified pursuant to Executive Order 13256 or that the disclosure of such information would be detrimental to the national security.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read 'D. Coombs', is positioned above the printed name.

DAVID EDWARD COOMBS
Civilian Defense Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison.)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**Prosecution Response
to Defense Motion
for Specific Instructions:
the Specification of Charge I**

6 July 2012

RELIEF SOUGHT

The Government respectfully requests that the Court deny the Defense Motion for Specific Instructions: the Specification of Charge I (Defense Motion). The Defense's proposed instruction transforms the Government's burden by requiring it to prove a specific intent to commit the charged offense, in contravention of the law, statutory text, and this Court's previous rulings. The Government requests that the Court adopt its proposed instructions in full and deny the Defense requested instruction for the specification of Charge I.

BURDEN OF PERSUASION AND BURDEN OF PROOF

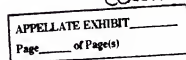
As the moving party, the Defense bears the burden of persuasion and must prove any factual issues necessary to decide this motion by a preponderance of the evidence. *See Manual for Courts-Martial* (MCM), United States, RCM 905(c) (2012).

FACTS

1. The Government stipulates to the facts in the Defense Motion. *See* Charge Sheet.
2. Knowledge is a recognized *mens rea* to provide an evil state of mind. *See* Appellate Exhibit LXXXI at 3.
3. Article 104 is a general intent crime. *See id.*
4. The general intent required by Article 104 is knowledge. *See id.*
5. Article 104(2) does not require a specific intent or motive to give intelligence to the enemy. *See id.*

WITNESSES/EVIDENCE

The Government does not request any witnesses be produced for this response. The Government respectfully requests that the Court consider the referenced Appellate Exhibits.



LEGAL AUTHORITY AND ARGUMENT

Criminal law distinguishes between an accused acting with knowledge that his conduct will create certain consequences and an accused acting with the specific purpose to effect those consequences. See *United States v. Bailey*, 444 U.S. 394, 404-05 (1980) (discussing differences of degree or punishment "between a person who knows that another person will be killed as the result of his conduct and a person who acts with the specific purpose of taking another's life") (citing *W. LaFave & A. Scott*, Handbook on Criminal Law § 28 at 196-97 (1972) (hereinafter "LaFave & Scott")). A person acts "knowingly" if he is aware "that the result is practically certain to follow from his conduct, *whatever his desire may be as to that result.*" *Bailey*, 444 U.S. at 404 (quoting LaFave & Scott at 196) (emphasis added); see Model Penal Code § 2.02(b). A person acts "purposefully," however, when "he consciously desires that result. . . ." *Bailey*, 444 U.S. at 404. Generally, knowledge corresponds with general intent and purpose corresponds with specific intent. See *id.* at 405 (citing LaFave & Scott at 201-02).

The Model Penal Code defines "intentionally" as "purposely," which equates to "with purpose" or "with design." See Model Penal Code §§ 1.13(11)-(12), 2.02(2)(a)-(b) (defining "purposely" as desiring to cause a specific result and "knowingly" as awareness that the conduct is practically certain to cause a result); see also *United States v. Nielson*, 471 F.2d 905, 908 (9th Cir. 1973). Moreover, "knowingly and intentionally" used in conjunction denote specific intent. See *Nielson*, 905 F.2d at 908 (affirming instructions describing "knowingly and intentionally" as a specific intent). Conversely, a "knowingly" standard simply requires awareness that a result is likely to follow, not a desire to effect that result. See *United States v. Springer*, 58 M.J. 164, 169 n.2 (C.A.A.F. 2003) (citing *Katz v. United States*, 389 U.S. 347, 351 (1967); Model Penal Code § 2.02(2)(a)).

I. ARTICLE 104 REQUIRES KNOWLEDGE AND NOT PURPOSE

The Specification of Charge I (the specification), alleging a violation of Article 104(2), requires the Government to prove that the accused knowingly gave intelligence to the enemy through indirect means. See Appellate Exhibit LXXXI at 3; Charge Sheet. Under Article 104, the Government must prove that the accused had actual knowledge that he was giving intelligence to the enemy through indirect means. See MCM pt. IV, ¶ 28c(5)(c); *United States v. Olson*, 20 C.M.R. 461, 464 (A.B.R. 1955). Actual knowledge constitutes a general intent. See Appellate Exhibit LXXXI at 3 ("The general intent required by Article 104 is knowledge."). Furthermore, actual knowledge constitutes the recognized *mens rea* to provide an evil state of mind. See *id.* The Government does not need to prove that the accused intended to give intelligence to the enemy through indirect means because Article 104 does not require specific intent. See *id.*

Actual knowledge simply requires awareness of the charged element. See *United States v. Adams*, 63 M.J. 223, 226 (C.A.A.F. 2006) (holding that actual knowledge can be satisfied by subjective awareness of high probability or deliberate ignorance).¹ Accordingly, the Government need only prove "knowingly" by demonstrating that the accused was aware that the enemy was practically certain to receive intelligence as a result of the charged acts. See *Bailey*,

¹ Article 86 requires actual knowledge. MCM pt. IV, ¶ 10c(2)

supra; Olson, 20 C.M.R. at 464 (deciding that Article 104 requires a general evil intent). Any intention, purpose, design, or desire is only required under a specific intent and not under the general intent required for Article 104.² See Bailey; Olson, *supra*. Thus, the Government is not required to prove that the accused desired the specific result of the enemy's receipt of intelligence.

II. THE PROPOSED DEFENSE INSTRUCTION INCORRECTLY REQUIRES SPECIFIC INTENT

The Defense's proposed instruction requiring the Government to prove specific intent is improper. The Defense uses its request for instructions to raise anew its contention that, as charged in this case, Article 104 requires the Government to prove a specific intent to commit the offense. See Appellate Exhibit LXII ¶ 8 (claiming that "no prosecution under Article 104(2) has been maintained without an allegation that the accused *intended* to give intelligence to, or communicate with, the enemy in some way") (emphasis added). For example, the Defense attempts to increase the standard from a general intent to a specific one by requesting a purpose standard. See Defense Motion ¶ 1 ("That is, the accused must have used the third party for the *purpose* of giving intelligence to the enemy") (emphasis added); *id.* at ¶ 7 ("In other words, the Government must prove that the accused used the third party for the *purpose* of giving intelligence information to the enemy.") (emphasis added). Additionally, the Defense attempts to inject a specific intent standard by requesting an "intentionally" standard. See *id.*; Defense Requested Instruction: Article 104 (Requested Instruction) at 2. Simultaneously, the proposed Defense instruction describes a "knowingly" general intent as insufficient. See Requested Instruction at 2 ("Providing intelligence to a third party with reason to believe that the enemy . . . would likely receive it, is insufficient."). Furthermore, the Defense improperly inserts a specific intent requirement into its definition of "indirect means" by requiring a desired purpose that the information be conveyed to the enemy by an intermediary. See Requested Instruction at 2 ("Absent an intention that the intermediary convey the information to the enemy, the accused's communication with a non-enemy individual or entity is not an "indirect" communication with the enemy regardless of whether an enemy ultimately was able to receive the substance of the information that the accused provided to the non-enemy."). In sum, the Defense instruction plainly contradicts the law and this Court's previous ruling on the Defense Motion to Dismiss the Specification of Charge 1.

"Knowingly and intentionally" sets a higher standard than "knowingly" and its exclusion from Article 104's language is notable because it is explicitly used elsewhere in the UCMJ. The drafters chose to employ the "knowingly and intentionally" standard in the MCM for noncompliance with procedural rules under Article 98(2), UCMJ; however, the drafters declined to implement this same standard for Article 104. See MCM pt. IV, ¶ 22a(2) (2012); see also MCM pt. IV, ¶ 30c(5) (requiring proof of a specific intent to prove a charge of spying under Article 106). Moreover, the Defense aptly observes that its proposed "knowingly and intentionally" standard sets a different and higher standard than the "knowingly" standard

² Indeed, the higher standard of specific intent is appropriate for the more serious charge of treason. See *Haupt v United States*, 330 U.S. 631, 641-42 (1947) (holding that jury should determine whether the accused intended to indulge his disloyal son or specifically injure the United States).

required for general intent under Article 104. See Defense Motion ¶ 26 (describing “knowingly and intentionally” as being “friendlier” to an accused).³ The Government agrees that “knowingly and intentionally” is a higher standard, but the Government disagrees that this higher standard is appropriate where it requires adding a term explicitly omitted from the plain text of Article 104 but included as an element of Article 98(2). See MCM pt. IV, ¶ 28c(5)(c) (2012); see also Section III, *infra*.

Moreover, the Defense’s discussion of the crime of arson fails to justify changing the general intent required to a specific intent. The Defense correctly notes that arson requires general intent in military justice; however, that intent is “willful and malicious,” which merely requires an intent greater than negligence. See *United States v. Acevedo-Velez*, 17 M.J. 1, 7 (C.M.A. 1983) (deciding that voluntary intoxication is not a valid defense because arson is not a specific intent crime). Arson is a separate crime requiring a different intent. Therefore, any comparison provides no insight into the charge of aiding the enemy.

III. THE MILITARY COMMISSIONS ACT AND COMMON LAW OF WAR DO NOT SUPPORT A “KNOWINGLY AND INTENTIONALLY STANDARD” IN THIS CASE

The Military Commissions Act comparison made by the Defense fails because Congress explicitly chose to add the “knowingly and intentionally” standard to Offense 26, yet the Drafters declined to change the language of Article 104 to include the “knowingly and intentionally” standard in both 2008 and 2012. See MCM pt. IV, ¶ 28c(5)(c) (2008); MCM pt. IV, ¶ 28c(5)(c) (2012). In fact, Congress further heightened the requirements of Offense 26 in comparison to Article 104 by adding a loyalty element. See 10 U.S.C. § 950t(26) (requiring, among other elements, a “breach of an allegiance or duty to the United States”). Additionally, the name of the offense cited by the Defense, “Wrongfully Aiding the Enemy,” also indicates an increased standard. Here, the accused is charged with aiding the enemy, not “wrongfully” aiding the enemy. Similarly, the common law of war cited by the Defense discusses the elements of wrongfully aiding the enemy, an offense for which the accused is not charged.⁴ Ultimately, the entire comparison is irrelevant because the offense cited by the Defense pertains to military commissions for unprivileged alien belligerents and not Soldiers who aid the enemy and are subject to courts-martial under the Uniform Code of Military Justice. See n. 3, *supra*.

³ Offense 26 is a charge for “Wrongfully Aiding the Enemy” as established by the Military Commissions Act of 2009, which establishes procedures governing the use of military commissions to try alien unprivileged enemy belligerents for violations of the law of war. See 10 U.S.C. § 948b(a) (2012). In responding to the Defense’s hypothetical situation where a terrorist’s acts are potentially evaluated under a “friendlier” *mens rea*, the Government notes that Soldiers, who owe a duty of loyalty to the United States, are consistently and widely held to a higher standard. Moreover, the Defense neglects to consider that the loyalty element, discussed *infra*, presumably would not apply to a terrorist because he would lack an ostensible allegiance or duty to the United States. Therefore, a terrorist would not be subject to Offense 26. Accordingly, the terrorist would not benefit from a “friendlier” *mens rea* than a Soldier charged with an Article 104 violation.

⁴ The Government also notes that the Defense cites the codification of the common law, which renders actual common law moot.

CONCLUSION

For the foregoing reasons, the prosecution respectfully requests that the Court deny Defense Motion for Specific Instructions: the Specification of Charge I.



ALEXANDER VON ELTEN
CPT, JA
Assistant Trial Counsel



JODEAN MORROW
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 6 July 2012.



JODEAN MORROW
CPT, JA
Assistant Trial Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

GOVERNMENT RESPONSE TO
DEFENSE REQUESTED
INSTRUCTION: SPECIFICATIONS
4, 6, 8, 12, AND 16 OF CHARGE II

6 July 2012

RESPONSE

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny giving the Defense Requested Instruction for Specifications 4, 6, 8, 12, and 16 of Charge II. The proposed defense instructions are confusing and incomplete in that they do not define necessary terms.

The United States objects to the defense instruction in its entirety, including any instructions that incorporate a mistake of fact defense before the presentation of evidence. The United States joins the defense in requesting a definition of "cost price" and "purloin." See Def. Mot. at 5, 6. The United States objects specifically to the following italicized portions:

Court Instructions¹

(1) That the property alleged to have been stolen, purloined, or knowingly converted, to wit: the Combined Information Data Network Exchange Iraq database containing more than 380,000 records, belonged to the United States government;

(2) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 5 January 2010, steal, purloin, or knowingly convert to his use or the use of another the named property;

(3) That the accused acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property.

Comment: These instructions do not accurately track either the Fifth Circuit Pattern Criminal Jury Instruction 2.33 or the Eighth Circuit Model Criminal Jury Instruction 6.18.641. See Enclosures 3 and 4 to the Government's Proposed Member Instructions. They appear to track the Eleventh Circuit Pattern Criminal Jury Instructions cited as authority by the defense, but the United States maintains that it makes more sense to group the *mens rea* (knowingly and willfully) with the act of "stealing, purloining, or converting." See Government's Proposed Member Instructions.

¹ The United States has the same objection to the instructions for all the 18 U.S.C. § 641 specifications at issue.


Court Definitions

[If stealing is charged]: To steal money or property means to take someone else's money or property without the owner's consent with the intent to deprive the owner of the value of that money or property.

[If purloined is charged]: To purloin is to steal with the element of stealth, that is, to take by stealth someone else's property without the owner's consent with the intent to permanently deprive the owner of the value of that property.

[If conversion is charged]: To knowingly convert property means to exercise control over the property in an unauthorized manner in a way which seriously or substantially interferes with the government's right to use and control its own property, knowing that the property belonged to the United States, and knowing that such use was unauthorized. Mere misuse of the property is not enough for you to find that the accused knowingly converted it. Rather, you must find that such misuse seriously or substantially interfered with the government's ownership rights in that property.

Comment: Stealing, purloining, and converting are all charged. See Charge Sheet. Inaccurate and misleading statement of the law in its entirety. To "steal" does not mean to take someone's property with the intent to deprive the owner of the value of that property. Similarly, "purloin" is also not linked to the intent to permanently deprive the owner of the value of the property. See *United States v. Morissette*, 342 U.S. 246, 270 (1952) ("Stealing...is commonly used to denote any dishonest transaction whereby one obtains that which belongs to another, and deprives the owner of the rights and benefits of ownership, but may or may not involve the element of stealth usually attributed to the word purloin."); Enclosure 4 to the Government's Proposed Member Instructions ("To 'steal' or 'convert' means the wrongful taking of property belonging to another with intent to deprive the owner of its use or benefit, either temporarily or permanently."); Enclosure 1 to the Government's Proposed Member Instructions. Additionally, in the "conversion" instruction, the United States is not required to prove that the accused "knew" that the property belonged to the United States, only that he knew that he property was not his. See Enclosures 3 and 4 to the Government's Proposed Member Instructions.


JUDEAN MORROW
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 6 July 2012.


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

Wget

“Wget” is a freely available network utility used to retrieve files from a web server using Hyper Text Transfer Protocol (HTTP) and File Transfer Protocol (FTP), two widely-used Internet protocols. *See* Enclosure 1. Wget can be used as a “web crawler” by extracting resources linked from web pages and downloading them in sequence, repeating the process recursively until all the pages have been downloaded or a maximum recursive depth specified by the user has been reached.¹ In other words, Wget can be used to rapidly mine data from websites. *See* Enclosure 2, at 131. During the Article 32 investigation, the United States presented evidence that the accused added Wget to his Secret Internet Protocol Router Network (SIPRNET) computer and used the program to access and harvest more than 250,000 Department of State diplomatic cables from the Net-Centric Diplomacy (NCD) website. *See* Enclosure 3. Wget was not authorized software for Army computers. *See* Enclosure 2, at 126. In order for a person to access and obtain a diplomatic cable on the NCD website, the person has to individually “click” or “save” the diplomatic cable after searching for the cable or navigating to the cable in some manner.

WITNESSES/EVIDENCE

The United States requests this Court consider the previous pleadings filed by the parties on this issue, Enclosures 1-3, and Appellate Exhibit CXXXIX.

LEGAL AUTHORITY AND ARGUMENT

The defense argues, again, that the United States has failed to allege the accused “exceeded authorized access” within the meaning of 18 U.S.C. § 1030(a)(1) because the accused “was authorized to access each and every piece of information he allegedly accessed.” Def. Mot. at 4. The defense argument has no merit. The Government’s theory for Specification 13 of Charge II – that the accused “exceeded authorized access” in violation of 18 U.S.C. § 1030(a)(1) when he obtained the information at issue using an unauthorized program – is a valid application of the statute, even as restricted by this Court’s ruling adopting the interpretation favored by the *Nosal* court.

I. THE GOVERNMENT’S THEORY IS CONSISTENT WITH THE HOLDING OF THE NINTH CIRCUIT IN *NOSAL*.

Nosal stands for the proposition that the term “exceeds authorized access” is limited to violations of restrictions on *access* to information, and not restrictions on its *use*. *Nosal*, 676 F.3d at 863-64; Appellate Exhibit CXXXIX, at 9. The proper inquiry in this case, therefore, is whether and to what extent there was a violation of an “access restriction” to the diplomatic cables at issue in Specification 13 of Charge II. *See* Charge Sheet. The defense argument, in essence, is that there was no access restriction to the information because the accused was “authorized to access each and every piece of information he allegedly accessed.” Def. Mot. at

¹ *See* <http://en.wikipedia.org/wiki/Wget>.

4. In the defense's view, the manner in which the information is downloaded is irrelevant. See *id.* However, the manner in which one accesses information is relevant to whether or not an individual "exceeds authorized access" under 18 U.S.C. § 1030(a)(1). The authority to access information cannot be meaningfully separated from the manner in which one does so. An individual's "authority" to do practically everything is limited by specific circumstances or by the scope of that authority, and this case is no different. See, e.g., *United States v. Khamsouk*, 57 M.J. 282, 304 (C.A.A.F. 2002) (discussing that apprehension under the guise of surveillance for purpose of obtaining evidence exceeds the scope of an arrest warrant). To hold otherwise would be to ignore the plain meaning of the statutory text and this Court's ruling adopting the narrow meaning of "exceeds authorized access" favored by *Nosal*. Additionally, the practical effect of adopting the defense position would be to further narrow "exceeds authorized access" into oblivion.

An individual "exceeds authorized access" under the CFAA and 18 U.S.C. § 1030(a)(1) when the individual "access[es] a computer with authorization and...use[s] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The renewed defense motion argues that a person exceeds authorized access only when he "obtains or alters information that he is not authorized to obtain or alter." Def. Mot. at 5. Consequently, "if a person is authorized to access certain files, the use of a program like Wget to download those files cannot change the fact that the person is still authorized to access those same files." Def. Mot. at 12. In short, the defense recycles the same argument they set forth in their original motion—that an accused "exceeds authorized access" to a computer only when he or she uses authorized access to a computer to obtain or alter information that he or she is never entitled to obtain or alter. See Def. Mot. at 3. This interpretation – that the manner of access is irrelevant – ignores common sense, the plain meaning of the statutory text, and the purpose of the statute itself.

The defense argues that the Government's interpretation still relies heavily on the word "so" in the statutory definition of "exceeds authorized access." See Def. Mot. at 8-9. While true that the word "so" indicates that "the manner" matters, the *Nosal* court helpfully addressed this issue in their decision rejecting the Government's theory that the defendant in that case "exceeded authorized access." While discussing the Government's interpretation of the word "so" in the statutory definition, the court indicated that the Government's reasoning failed because the word "has meaning even if it doesn't refer to use restrictions." *Nosal*, 676 F.3d at 858. The court explained:

Suppose an employer keeps certain information in a separate database that can be viewed on a computer screen, but not copied or downloaded. If an employee circumvents the security measures, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not 'entitled so to obtain.' Or, let's say an employee is given full access to the information, provided he logs in with his username and password. In an effort to cover his tracks, he uses another employee's login to copy information from the database. Once again, this would be an

employee who is authorized to access the information but does so in a manner he was not authorized 'so to obtain.'

Id.

In short, even the *Nosal* court never went so far as to hold that the manner in which one accesses information is irrelevant to a determination of whether an accused "exceeds authorized access" within the meaning of 18 U.S.C. § 1030(a)(1) and (e)(6). The examples above, along with the narrow scope of the court's holding (restrictions on access to information, not restrictions on its use), clearly demonstrate that the court considered "the manner" relevant. The obvious common thread in both of the *Nosal* court's hypotheticals is that the potential defendant has access to the information. The defendants were entitled or authorized to view the information in a specific way. The defendants only access information in excess of authority when they access the information in some unauthorized manner. Ultimately, if the court thought the issue was black and white – if an individual has access to the information in some capacity, then they cannot exceed authorized access – they would have articulated that draconian concept more clearly. While the Government concedes this jaunt is mostly dicta—it is important because it indicates the court's thinking on this matter. Accordingly, because the Government's theory has unquestioned support in the dicta of *Nosal* and the court's narrow holding, the Government's theory is a valid application of the statute.

II. THE GOVERNMENT'S THEORY IS CONSISTENT WITH THE LANGUAGE OF THE 1996 LEGISLATIVE HISTORY.

As noted by the Court in Appellate Exhibit CXXXIX, Congress amended § 1030(a)(1) in 1996. See Appellate Exhibit CXXXIX, at 6; S. Rep. No. 104-357 (1996). The Court informed the parties that it would craft instructions for defining "exceeds authorized access" using the language in the legislative history in 1996. *Id.* at 9. To the extent that the language in the 1996 legislative history contributes in any meaningful way to a determination of what constitutes "exceeding authorized access" within the meaning of § 1030(a)(1), the Government's theory of criminal liability is consistent with the language.

The 1996 amendments to § 1030(a)(1) brought the language of the statute in line with 18 U.S.C. § 793(e). As the Senate report explained:

Although there is considerable overlap between 18 U.S.C. 793(e) and section 1030(a)(1), as amended by the NII Protection Act, the two statutes would not reach exactly the same conduct. Section 1030(a)(1) would target those persons who deliberately break into a computer to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments. In other words, unlike existing espionage laws prohibiting the theft and peddling of government secrets to foreign agents, section 1030(a)(1) would require proof that the individual knowingly used a computer without authority, or in excess of

authority, for the purpose of obtaining classified information. In this sense then, it is the use of the computer which is being proscribed, not the unauthorized possession of, access to, or control over the classified information itself.

S. Rep. No. 104-357, at 6 (1996).

The defense is singularly focused on Congress' explanation that § 1030(a)(1) targets those persons who "deliberately break into a computer." See Def. Mot. at 10. However, the Government does not allege the accused hacked "into the computer to obtain information he was not authorized to obtain." Def. Mot. at 10. Instead, he accessed a computer with authorization and exceeded that authorization by circumventing procedures and using an unauthorized program to obtain information—he "hacked" the information. When Congress inartfully summarized § 1030(a)(1) in the 1996 legislative history, they were clearly referring to the "without authorization" prong of § 1030(a)(1). See 18 U.S.C. 1030(a)(1) ("Whoever having knowingly accessed a computer without authorization...."). There is no other logical explanation, because "exceeds authorized access" under 1030(e)(6) necessarily assumes that the individual has accessed a computer with authority in the first place—it criminalizes the "insider" with rights or privileges who misuses a computer. See Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1662 (2003) [hereinafter Kerr, *Cybercrime's Scope*]; *Nosal*, 676 F.3d at 858. Thus, that particular phrase ("deliberately break into a computer"), is misleading if used solely as a basis for defining "exceeds authorized access."

On the other hand, if "deliberately break into a computer" is merely a guiding light in making sense of the purpose of the statute as whole, it contributes to our understanding of "exceeds authorized access." As this Court recognized after considering the legislative history, "the statute is designed to criminalize electronic trespassers and computer hackers." In other words, the statute is designed to criminalize individuals who circumvent or bypass some code-based restriction. See generally Kerr, *Cybercrime's Scope*, at 1600 (using trespassing, hacking, and "bypassing code-based restrictions" somewhat interchangeably). Accordingly, the Government's theory is entirely consistent with the legislative history and this Court's ruling. In order for a person to access or obtain a diplomatic cable on the NCD website, the person has to individually "click" or "save" the diplomatic cable after searching for the cable or navigating to the cable in some manner. As the evidence will show, the accused bypassed the ordinary method of accessing information by adding unauthorized software to his SIPRNET computer and using that software to rapidly harvest or data-mine the information. Wget was not available on the computers used by the accused or authorized as a tool to download the information. See Def. Mot. at 3. Thus, the accused violated a restriction on access to the information – he bypassed a code-based restriction – by using Wget to obtain the cables in batches.

Additionally, the Government's theory for Specification 13 is consistent with the language of the legislative history because it is anchored to the accused's egregious use of unauthorized software on a government-owned SIPRNET computer. As Congress noted in discussing the difference between §§ 793(e) and 1030(a)(1), "it is the use of the computer that is being proscribed, not the unauthorized possession of, access to, or control over the classified

information itself.” Section 793(c) is focused on the unauthorized possession and transmission of the information, while § 1030 is focused on the misuse of a computer. Wget, despite the wildly erratic defense argument to the contrary, is focused on the use of the computer, not the use of the information.² See Def. Mot. at 10 (“[T]he Government is attempting to use a violation of a use restriction under the AUP – the installation and use of Wget – to show that PFC Manning exceeded authorized access.”). As such, the Government’s theory is clearly consistent with the language of the 1996 legislative history.

III. THE GOVERNMENT’S PROPOSED INSTRUCTIONS BALANCE COMPETING THEORIES AND INCORPORATE *NOSAL* AND THE LEGISLATIVE HISTORY.

The Government’s proposed member instructions for Specification 13 of Charge II, and specifically the term “exceeds authorized access,” complies with this Court’s ruling on the original Defense Motion to Dismiss Specifications 13 and 14. See Government’s Proposed Member Instructions, at 18-22. First, the United States proposed that the Court instruct the fact finder that “Section 1030(a)(1) is focused on the individual’s use of a computer.” *Id.* at 19; see Appellate Exhibit CXXXIX, at 9 (“The Court shall craft instructions...using the language in the legislative history in 1996.”). The United States incorporated language directly from the legislative history. Additionally, the United States proposed the following instruction for “exceeds authorized access”:

The term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter. “Exceeds authorized access” under § 1030(a)(1) is limited to violations of restrictions on access to information, and not restrictions on its use. In deciding whether the accused “exceeded authorized access” to the State Department cables at issue, you may consider all the evidence introduced at trial, including any evidence concerning the use of unauthorized software to obtain the cables and any access limitations or restrictions to the State Department cables, or lack thereof, on the SIPRNET. The words “access” and “use” are commonly used and commonly understood words.

See Government Proposed Member Instructions, at 20.


The above instruction incorporates the statutory definition of “exceeds authorized access” under § 1030(e)(6), the holding of the court in *Nosal*, and the competing theories of the Government and the defense. In other words, the instruction allows the fact finder to determine whether and to what extent there was an “access restriction” to the State Department cables. It

² Arguably, the language of the 1996 legislative history – that § 1030(a)(1) would require proof that an individual knowingly used a computer in excess of authority for the purpose of obtaining classified information – is also fully compatible with the Government’s previous theory that the accused “exceeded authorized access” when he violated a purpose-based restriction on access.

presents a shortened version of the Government theory (use of unauthorized software) and the defense theory (lack of limitations or restrictions on the SIPRNET). The instruction balances both theories and should be adopted by this Court in full.

CONCLUSION

The United States respectfully requests this Court DENY, in part, the Renewed Motion to Dismiss for Failure to State an Offense. For the reasons stated above, Specification 13 of Charge II adequately states an offense punishable under 18 U.S.C. § 1030(a)(1). In the alternative, the United States requests the Court defer ruling on this motion until the presentation of evidence. The United States maintains that its theory of criminal liability for Specification 14 is dependent upon instructions by the Court.


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 6 July 2012.


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

3 Encls

1. Forensic Report Excerpt
2. Article 32 Testimony, SA David Shaver
3. Continuation Sheet, DD Form 457, pp. 27-32

Appellate Exhibit 188
Enclosure 1
1 pages
ordered sealed for Reason 6
Military Judge's Seal Order
dated 20 August 2013
stored in the original Record
of Trial

9 SPECIAL AGENT DAVID SHAVER, Civilian, was called as a witness
10 for the prosecution, was sworn, and testified in substance as
11 follows:
12

13 DIRECT EXAMINATION
14

15 Questions by assistant trial counsel 1:
16

17 I work for the Army Computer Crimes Investigative Unit. I
18 began working for them in 1999, at the time I was in the
19 military as a CID agent and an investigator. I am in a
20 supervisory position now, I am the Special Agent in charge of
21 the digital forensics and research branch. Our job is to
22 conduct examinations of digital media in support of CCIU cases.
23 The primary mission is to investigate any intrusion into any
24 Army computer worldwide, however we are tasked to do other
25 stuff.
26

27 I have received training from several locations. The first
28 would be the Law Enforcement Training Center, in Glencoe,
29 Georgia; the Defense Cyber Crime Center in Maryland, and I have
30 been trained on various commercial products as well. Products
31 such as a forensic product called ENCASE, which is a computer
32 forensic program that allows you to examine digital media. I
33 received training on Windows, Unix, Linux, and Macintosh. I
34 hold several certifications; I am a certified computer crime
35 investigator, an ENCASE certified examiner, A+ and net plus.
36 The A+ certification is a hardware-based certification. Net
37 Plus is a network-based certification. I have published
38 articles related to the field of computer forensics. I co-
39 authored a chapter on Windows forensics in the handbook of
40 digital forensics investigations. I have given several
41 scholarly presentations. A virtual machine is where we
42 developed a process to take a forensic image and turn it into a
43 virtual machine on your host computer. By using a virtual
44 machine you can gain the perspective of examining the computer
45 as a subject has used it.
46

1 I was notified of this case in late May of 2010, I examined
2 pieces of media related to this case. The first things I
3 examined were two SIPR computers. They were his primary and
4 secondary computers. An IP is an Internet protocol address,
5 which is a set of numbers that are unique to each computer. I
6 am familiar with Intelink, Intelink is Google of the SIPRNET. I
7 examined Intelink logs, those log files ranged from October 2009
8 until May 2010. From the logs I was able to obtain the majority
9 of the activity that happened on the computer. I identified
10 some kind of query and then I ran a search against log files for
11 that query, after that I verified it as well. I put them into
12 an Excel spreadsheet for ease of review. I noticed that there
13 were a lot of searches that seemed out of place, the keyword
14 searches that he was using seemed out of place for his job.

15
16 [The trial counsel published screenshot documents for the
17 witness to view on a monitor.]

18
19 That is a screenshot of the Excel spreadsheet that I
20 created called keywords. It is a filtered spreadsheet of the
21 keyword searches for WikiLeaks. From November 2009 through May
22 2010, I found over one hundred searches for WikiLeaks under PFC
23 Manning's profile. This is a different screenshot from that
24 same Excel spreadsheet; this time we filtered on the keyword
25 Iceland. The first search for Iceland was 9 January 2010, it is
26 only filtered on the keyword Iceland and this came from PFC
27 Manning's profile. This is another screenshot from the same
28 Excel spreadsheet; this time I filtered on the keyword
29 retention, and it was searching for the retention of
30 interrogation videos. That search was done 28 November 2009,
31 that was the first time that he searched for it.

32
33 The Intelink program also the captured the use of a WGET
34 program to download a large number of files. WGET is a command
35 line utility to download files from a Web server. Command line
36 means it is non graphical, meaning that you have to open up a
37 command prompt and then you are able to type the commands, it is
38 like a DOS program. WGET is not a standard program on an Army
39 computer. As part of my job to investigate intrusions, I get a
40 list of authorized software and WGET is not on that list. The
41 first time that I saw PFC Manning access WGET was March of 2010.
42 This is another portion of the screenshot of the Excel
43 spreadsheet that I created for Intelink. This portion is
44 filtered on the word WGET. The server in question was a
45 SharePoint server, so it stores files by ID number, it is a
46 database. The numbers beside the file ID number represent the
47 action that was taken for the searches, if a document was

1 downloaded, if the search came back, file not found, things of
2 that nature. There were over seven hundred examples of the
3 computer using WGET commands for the month of March pertaining
4 to JTF Guantánamo Bay detainee suspects. I know this because I
5 downloaded the same documents using the same program, and I used
6 the same path. And I know that they were the same documents
7 that were on the WikiLeaks website because I compared the two.

8
9 When we conduct a forensic examination, the first thing we
10 do is we verify the hashes, that the acquisition matches their
11 verification hashes. We scan the computer for antivirus and
12 then we generally conduct keyword searches. So when I began my
13 forensic examination the first thing that I look at is the hash
14 values of the images. The hash values have to match because if
15 they don't match, then there is a problem with the image. The
16 hash values of the acquiring image and of the image that I
17 looked at matched. The primary tools that I use to examine
18 computers are ENCASE. I plug keywords into ENCASE and then I
19 search for keywords, I search both the allocated and the
20 unallocated spaces. Allocated space is places on the hard
21 drive, files that are created that you can see, such as a Word
22 document or e-mail. Unallocated space is places on the hard
23 drive which have not been used yet or it may contain deleted
24 files. I was also able to recover deleted files, because
25 deleted files are still on the hard drive until something is
26 written over top of them.

27
28 With respect to the [dot] .22 computer, I was given a
29 series of chat logs, they were statements concerning the
30 Department of State, JTF Guantánamo Bay Cuba, things like that,
31 so that is where I started my keyword list. The chat logs were
32 collected from Mr. Lamo, I was looking for things that were
33 identified in the chat logs. I did a search in the allocated
34 space, and I found four complete JTF Guantánamo Bay, Cuba
35 detainee assessments. I knew that they were detainee
36 assessments because I read them. They were under PFC Manning's
37 user profile. This computer had two web browsers on it,
38 Internet Explorer and Firefox. The configuration for the
39 Internet explorer web browser was a standard Army configuration
40 where the user could not clear the Internet history. The
41 Internet history on a Windows computer would be stored in a file
42 called index.dat. It stores Internet information as well as
43 files that were opened up on the computer. The other web
44 browser on the computer was Firefox, it was configured to have
45 Intelink as its homepage and to auto start private browsing when
46 it started.

1 I found a [dot] .zip file under PFC Manning's user profile
2 and inside of it were over ten thousand complete Department of
3 State cables, web pages. I also found an Excel spreadsheet, it
4 was a spreadsheet with three tabs, the first tab was WGET, the
5 second tab was 0310-0410, and the third tab was 0510. In the
6 second tab was Department of State message record numbers that
7 were published between March 2010 until April 2010, they were
8 sequential, whoever did this was obviously keeping track of
9 where they were, the first number was 251,288, and then a
10 sequential number after that. To my knowledge WikiLeaks has
11 released 251,287 cables. On a third tab it was all of the
12 Department of State cables that were published in May 2010. It
13 was just message record numbers not the full cable.
14

15 There was a WGET tab in there as well, it was over ten
16 thousand message record numbers, the second column was the
17 command line using WGET that downloaded that message record
18 number from the Department of State net centric server. The
19 first column is the message record number, and there's about ten
20 thousand there. The next column is a script, it's a
21 mathematical computation basically saying take everything that
22 is in column A and put it in column B, but in the right path.
23

24 The Investigating Officer stated that it would be easier to
25 understand if they were able to see the document that the
26 witness was talking about.
27

28 The trial counsel informed the Investigating Officer that
29 although the document is not classified it is currently marked
30 as classified and that is the reason why he was not able to
31 display the document in open court.
32

33 The defense counsel objected to all parties viewing the
34 document from the jury box stating that it would be better for
35 everyone to recess and reconvene tomorrow when the problem is
36 fixed.
37

38 The trial counsel stated that his direct line of
39 questioning would not take that much longer and requested to
40 continue with the questioning of this witness.
41

42 The Investigating Officer stated that it would be better
43 for all if the trial counsel just continued with his line of
44 questioning explaining the document in detail.
45

1 The trial counsel gave the document number to the
2 Investigating Officer so that he would be able to review it once
3 he went back to his chambers.
4

5 **The direct examination by Assistant Trial Counsel 1 continued as**
6 **follows:**
7

8 In Column B it is an Excel formula, to take what is in
9 Column A and put it in to a script so it could identify the
10 file. After you have all of column B filled, you would be able
11 to copy that column as text and put it in a batch file; and run
12 the batch file in a command script. There were about ten
13 thousand commands in that batch, and I saw those message record
14 numbers on the left, they were downloaded into the original zip
15 file I discussed earlier.
16

17 This is all under PFC Manning's user profile. In the
18 Windows prefetch folder there were several instances of WGET
19 being run. Prefetch is a Windows feature to speed up the
20 computer. The computer will identify programs that you use on a
21 regular basis, so the next time you run the program it will load
22 quicker. You can run that program WGET at the same time from
23 various locations; that way you will be able to download a lot
24 of files simultaneously.
25

26 WGET was in PFC Manning's profile, it appeared 4 May 2010.
27 It was not the first time that he used that file because there
28 were prefetch files predate that. Within the Windows temp
29 folder there were two files, these files each contained
30 approximately 100 complete Department of State cables, these
31 files were in CSV format and they contained a base 64 encoded
32 version of the cables. A CSV file is a Comma Separated Value.
33 It is just a way of moving files from one database to another.
34 Base 64 is an encoding scheme, it transforms data and documents
35 into a different format. Someone would do that to streamline
36 the process of taking the cables out; it took away all the
37 punctuation, all the spacing, and just put the information in
38 straight base 64. I found evidence in the unallocated space; I
39 identified thousands of the State Department complete cables.
40 They were unclassified or secret. They were not all complete.
41

42 Other information that I found relating to detainee
43 information was ISNs, the Internment Serial Numbers, which are a
44 unique pattern of characters. I did a search for them and I
45 found hundreds of documents with that convention. The ISN is
46 the internment serial number and is used as an identifier. I

1 found ISNs on PFC Manning's computer. They were found in the
2 index.dat file.

3
4 I am familiar with the charges and specifications. I found,
5 in the allocated space, the movie, actually several movies; one
6 was the released version from Wikileaks and there was another
7 version which appeared to be the source file for it. The first
8 instance of that video being there was March, through
9 examination of the restore points I was able to determine that.
10 Restore point is another Microsoft feature and they are created
11 when an operating system is updated or program is installed so
12 if there's a problem with the computer you can go back in time
13 and get your computer to work again.

14
15 I do recognize that image, this is a screenshot of the
16 ENCASE program displaying from left to right the filename which
17 is the restore point, the middle column shows you the 12 July
18 2007 CZ engagement zone file was present under PFC Manning's
19 profile. I believe the first time it was viewed was 2 March
20 2010. There were no restore points before the month of March
21 due to the fact that the computer had problems and it was
22 reimaged prior to that.

23
24 I found information relating to an investigation done on a
25 military operation in Afghanistan. Within the index.dat file
26 there were hundreds of files which appeared to be part of the
27 incident, and I recovered deleted PDFs and JPEG images
28 pertaining to the Gharani incident. That is an image of the
29 index.dat which I put into an Excel spreadsheet for ease of
30 viewing. It is just a snippet of it. From left to right you
31 have the date column and to the right of that you have the URL,
32 what sites were visited. The date is April 10, 2010, says
33 Bradley.Manning as a file. That means that it is a file on the
34 computer not a website and then you continue reading and it
35 gives the path. It appears that somebody using the
36 Bradley.Manning user profile downloaded a large number files
37 concerning the Farah incident and at the end created a
38 Farah.zip. All of this was time sequential. In unallocated
39 space I recovered numerous JPEG images and PDF files, they
40 appear to be from presentations, screenshots of presentations,
41 pictures from aircraft, reconnaissance over the combat zone.

42
43 [The witness was temporarily excused, duly warned, and
44 withdrew from the courtroom.]

45
46 [The Article 32 hearing recessed at 1834, 18 December
47 2011.]

1
2 [The Article 32 hearing was called to order at 0934, 19
3 December 2011.]

4
5 The Investigating Officer called the hearing to order, and
6 stated that all parties present prior to the recess were once
7 again present.

8
9 **SPECIAL AGENT DAVID SHAVER, Civilian, was recalled as a witness**
10 **for the prosecution, was reminded that he was still under oath,**
11 **and testified in substance as follows:**

12
13 **CROSS-EXAMINATION**

14
15 **Questions by the civilian defense counsel:**

16
17 I did the computer forensics on both of the computers that
18 were sent to my office that PFC Manning used. I did not do a
19 bit by bit analysis of all the SIPR computers in the SCIF. I do
20 not know the total number of SIPR computers in the SCIF. I do
21 not know if the program WGFT was on the other computers.

22
23 WGFT is a program that is used for data mining, a key job
24 for analysts is to do data mining. Yesterday I stated that
25 WikiLeaks released over 250,000 cables. And during my analysis
26 I found diplomatic cables in the file called files.zip, that
27 file was found in allocated computer space. I did not compare
28 the cables that I found in the file with the cables that were on
29 the WikiLeaks website. None of those cables that I found in the
30 files.zip folder were on the WikiLeaks website. The computer
31 that I found these cables on was a SIPR computer. I was not
32 aware that analysts were directed to look at these cables. I
33 was not aware that no password was required to access these
34 files. I did not know that there was no prohibition for any
35 analyst to download these files.

36
37 Generally, you cannot date and timestamp things that are in
38 the unallocated space. And with unallocated space there is
39 nothing that you can tie to one particular user. I found the
40 video that has been called the Apache video; it was on one of
41 the SIPR computers. I did not know that the Apache video was a
42 topic of discussion among the analysts at FOB Hammer. I did not
43 know that these analysts were talking about and watching this
44 certain video back in December 2009. If a file has been deleted
45 and the space that was allocated and has been written over I
46 cannot find out what that file was. I testified that WGFT was
47 used to download hundreds of files onto the allocated space of

1 the computer. In the allocated space I found four detainee
2 assessments, and in the unallocated space I found zero.

3
4 **REDIRECT EXAMINATION**

5
6 **Questions by Assistant Trial Counsel 1:**

7
8 The cables in the files.zip folder were not released.

9
10 **OBJECTION**

11
12 The defense counsel objected to the line of questioning
13 stating it was cause for speculation.

14
15 The Investigating Officer overruled the defense's
16 objection.

17
18 **The redirect examination by the trial counsel continued as**
19 **follows:**

20
21 When the files.zip was created there was something wrong,
22 there was a problem with it, if a person using WinZip tried to
23 open it, it would not open because it was a corrupted file. So
24 you would need special tools in order to open the files in that
25 zip folder.

26
27 **OBJECTION**

28
29 The defense counsel objected stating the trial counsel was
30 asking leading questions.

31
32 The Investigating Officer sustained the objection.

33
34 **The redirect examination by the trial counsel continued as**
35 **follows:**

36
37 I did find files related to the Farah investigation in the
38 unallocated space. I found four detainee assessments in the
39 allocated space. I did find evidence of the detainee
40 assessments in the index.dat file folder. The detainees have a
41 unique naming system, the ISN, I looked for the pattern for that
42 and there were hundreds of those in the index.dat. The
43 index.dat file is a Microsoft file used to log all of the
44 websites and files viewed by the user.

45
46 **RECROSS-EXAMINATION**

1 **Questions by the civilian defense counsel:**

2
3 I was not able to open the form of file on unallocated
4 space. I testified that the files.zip folder was corrupted I
5 was not able to tell when it was corrupted.

6
7 The Investigating Officer closed the courtroom.

8
9 [The Article 32 hearing recessed at 1012, 19 December
10 2011.]

11
12 [The Article 32 hearing was called to order at 1016, 19
13 December 2011.]

14
15 The Investigating Officer opened the courtroom.

16
17 **SPECIAL AGENT DAVID SHAVER, Civilian, was called as a witness**
18 **for the prosecution, was sworn, and testified in substance as**
19 **follows:**

20
21 **DIRECT EXAMINATION**

22
23 **Questions by assistant trial counsel 1:**

24
25 An IP address is an Internet protocol address. It is a
26 unique set of numbers that is assigned to a computer so that it
27 can talk on the network. The [dot] .40 machine was the machine
28 that PFC Manning's user profile was on. That was his secondary
29 computer. I verified the acquisition and verification hashes,
30 the hashes matched. Then I scanned it with antivirus, then I
31 conducted my examination.

32
33 The configuration of this computer was that it was a
34 classified computer, a Windows operating system on the Army
35 domain. It has CD burning tools, it had Roxio that was
36 installed on the computer. Roxio is CD burning software. Roxio
37 was on the other computer, the [dot] .22 computer that also had
38 PFC Manning's user profile on it. USB ports were disabled for
39 storage, it is an Army policy. On both computers the USB ports
40 were disabled. When you burn a disk using Roxio, the CD has to
41 be named and it was named by date. This image is an artifact,
42 the naming of a CD that I burned when I re-created, I turned the
43 [dot] .22 computer into a virtual machine. A virtual machine is
44 a bit by bit image of a computer, it converts it to a running
45 computer within your computer which acts as a host, so it is
46 running virtually in the memory of the host computer. I wanted
47 to verify that a CD could be burned from this computer and so I

1 turned it into a virtual machine, logged on as a user and then I
2 burned a disc.

3
4 My investigative plan for the[dot] .40 computer was the
5 same thing as the [dot] .22, to see if there were any
6 Department of State cables, see if there were any Guantánamo Bay
7 detainee assessments on there. I approached it the same way.
8 In the unallocated space I located a deleted CSV file containing
9 over 100,000 complete Department of State cables, which had been
10 converted to Base 64 format. A CSV is a Comma Separated Value;
11 it is just a way of transferring data from one database to
12 another area. The utility of a CSV is a common format, and
13 between each field there is a comma. Base 64 is just a way of
14 encoding information, the benefit for it in this case would be
15 to remove all of the characters, all of the grammatical
16 characters. When something is base 64 encoded it looks like, to
17 the untrained eye, gibberish. I found more than 100,000 full
18 cables.

19
20 The image is a very small portion of the recovered CSV
21 file, and what I've done for this one is, to keep it presentable
22 in open court; I filtered it on some of the unclassified
23 Department of State cables. On the left, the first field would
24 be the numbers, the person who was doing this wanted to ensure
25 that he obtained all of them, so each one of them had a unique
26 number. The second field is the date of when it was published,
27 when the actual cable itself was published on the Department of
28 State server, this is the Message Record Number, MRN. A message
29 record number is how the Department of State labels their
30 cables. And to the right of that is the base 64 stuff that I
31 spoke of. There is a reverse process to decode base 64. It
32 presents the information in plain text. And I was able to
33 decode these cables.

34
35 I found this deleted CSV in unallocated space, but I could
36 not associate that with a user profile. You can decode manually
37 one at a time, but that would be very time-consuming and prone
38 to errors. Through scripting you can create an automated process
39 to decode for you in a very quick manner. I did not find a
40 script to decode it on this computer. I did not find any other
41 data sets on the [dot] .40 computer.

42
43 I do recognize that image, which is the warning banner for
44 the computers, [dot] .22 and the [dot] .40 computers. When you
45 first start the computer and try to log on, you are presented
46 with this warning banner. The first sentence states, "You are
47 accessing a US government (USG) information system that is

1 provided for US government authorized use only." When a user
2 first logs on to the computers that I examined, you're first
3 prompted with this warning screen and then you have to press
4 okay.

5
6 **CROSS-EXAMINATION**
7

8 **Questions by the civilian defense counsel:**
9

10 The CSV file that I just discussed was in unallocated
11 space, so I cannot say that it was PFC Manning that accessed
12 this information. I do not know whether usernames and passwords
13 were shared at the T-SCIF on FOB Hammer. The unallocated space
14 with the cables cannot be date and time stamped. I found this
15 information on a classified computer; there is nothing wrong
16 with this information being on a classified computer. I did not
17 find any forensic evidence that this information was sent to
18 anyone.
19

20 [The witness was temporarily excused, duly warned, and
21 withdrew from the courtroom.]

Continuation Sheet, DD Form 457, U.S. v. PFC Bradley E. Manning

indicates that PFC Manning provided the BE 22 PAX.wmv file to WikiLeaks and that file was the one that was placed on Mr. Katz's computer.

The evidence showed that in the context of his chats with Mr. Lamo concerning the State Department cables where he said, "it was forwarded to WL ... and god knows what happens now ... hopefully worldwide discussion, debates, and reforms,"¹¹⁶ PFC Manning had reason to believe that the information in this video could be used to the injury of the United States. PFC Manning had no need to access information concerning Afghanistan for his job,¹¹⁷ and he had no authorization to provide these documents to WikiLeaks, which was not authorized to receive it.

The evidence showed that this video was properly classified and remains classified.¹¹⁸

The evidence showed that 18 U.S.C. 793(e) exists and that PFC Manning's conduct in providing these records to WikiLeaks was prejudicial to good order and discipline and service discrediting.

I thus conclude that reasonable grounds exist to believe that PFC Manning committed the offense alleged in Specification 11 of Additional Charge II.

Additional Charge II, Specification 12 (Art. 134, UCMJ; 18 U.S.C. 641):

Law

In order to prove this offense, the government must establish the following five elements:

- (1) that at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 4 May 2010, the accused voluntarily, intentionally and knowingly stole, purloined, or converted a thing of value, to wit: the Department of State Net-Centric Diplomacy database containing more than 250,000 records belonging to the United States government to his use or to the use of another;
- (2) that the thing of value belonged to the United States and had a value in excess of One Thousand Dollars (\$1,000);
- (3) that the accused did so with intent to deprive the owner of the use or benefit of the thing of value so taken;
- (4) that 18 U.S.C. section 641 exists; and
- (5) that, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

¹¹⁶ Lamo Chat, IO Ex. 19(D), at 33.

¹¹⁷ Testimony of CPT Lim (stating PFC Manning had no need to access the CIDNE-Afghanistan database for his job)

¹¹⁸ Classification Review, Bates # 00376879-902.

Facts

The evidence showed that PFC Manning's primary SIPRNET computer contained, under his user profile, a file named "files.zip" in the "bloop" folder that had over 10,000 Department of State cables in .html web page format, and that over 4,000 of these cables were classified.¹¹⁹ A CD accessed on PFC Manning's personal computer containing files.zip was burned on 4 May 10.¹²⁰ The evidence showed that another document in the "bloop" folder, "backup.xlsx," was a spreadsheet with cables published in March, April, and May 2010.¹²¹ The tab in this spreadsheet including cables published in March and April 2010 started with a cable with number 251,288.

The evidence showed that PFC Manning's primary SIPRNET computer had a version of wget (software used to download files from a server) that was the same version found in the Department of State log files, the Intelink log files, and that was downloaded on a NIPRNET computer by the bradley.manning user profile.¹²² A user of PFC Manning's user profile on that NIPRNET computer did Google searches for WikiLeaks and wget.exe on 3 May 2010 and downloaded wget to that profile. A user of PFC Manning's user profile then transferred wget from the NIPRNET to SIPRNET on 4 May 2010, under PFC Manning's user profile.¹²³

The evidence showed that on 20 August 2011, WikiLeaks released 251,287 Department of State cables in unredacted form and made them available on the Internet.¹²⁴ While the evidence was that WikiLeaks did not release the cables in the files.zip folder,¹²⁵ the forensic examination found thousands of State Department cables in unallocated space on PFC Manning's primary SIPRNET computer, ranging in classification from unclassified to secret; many were complete, but many others were not.¹²⁶ Additionally, the forensic examination of PFC Manning's primary SIPRNET computer revealed that a deleted and partially overwritten file named "c:\Lost File\backup\farah.zip" was originally created on 10 April 2010 and contained 582 Department of State Cables, over 250 of which were classified.¹²⁷ The evidence showed the Department of State cables were in .csv format, a way of moving files from one database to another, and were Base64 encoded.¹²⁸ Analysis of PFC Manning's secondary SIPRNET computer and his personal computer also showed many Department of State cables that had been converted to Base64 and stored in .csv format.¹²⁹ Specifically, approximately 113,000 complete Department of State cables converted to Base64 were found in a deleted .csv file in Unallocated Clusters on PFC

¹¹⁹ Testimony of SA Shaver; PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 31.

¹²⁰ Testimony of SA Shaver.

¹²¹ PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 31; spreadsheet, at Bates # 00296982; Testimony of SA Shaver.

¹²² PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 37.

¹²³ Testimony of SA Shaver.

¹²⁴ Testimony of SA Bettencourt; Testimony of SA Shaver.

¹²⁵ Testimony of SA Shaver. SA Shaver also testified there was a problem with files.zip when it was created, and if a person using WinZip tried to open it, it would not open because it was a corrupted file, and one would need special tools to open the files in files.zip. Based on that testimony, it appears that WikiLeaks did not release the cables in files.zip because they could not open them.

¹²⁶ Testimony of SA Shaver.

¹²⁷ PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-II 0, at 34-36

¹²⁸ Testimony of SA Shaver.

¹²⁹ PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 36.

Continuation Sheet, DD Form 457, U.S. v. PFC Bradley E. Manning

Manning's secondary SIPRNET computer,¹³⁰ and evidence of Department of State cables published before March 2010 were found in Unallocated Clusters on PFC Manning's personal computer, including data appearing to have a .csv file structure listing Department of State cables with numbers preceding 251,287 in a format similar to the cables found on PFC Manning's primary SIPRNET Computer.¹³¹ Additionally, examination of Department of State cable message record numbers released by WikiLeaks identified 251,298 individual message record numbers; examination of PFC Manning's personal computer and his primary and secondary SIPRNET computers showed that they contained 83% of all the message record numbers released to WikiLeaks.¹³²

This evidence, taken together, leads to a conclusion that the 251,287 files released by WikiLeaks were provided to WikiLeaks by PFC Manning.

The evidence showed that in his chats with Mr. Lamo concerning the State Department cables, PFC Manning said, "it was forwarded to WL ... and god knows what happens now ... hopefully worldwide discussion, debates, and reforms ... I want people to see the truth... regardless of who they are... because without information, you cannot make informed decisions as a public,"¹³³ which indicates that that he converted this database to his own use or the use of another in that he wanted to make this information public and thus deprive its owner, the United States, of its use or benefit. While there was evidence that PFC Manning had the authority to access diplomatic cables for his job,¹³⁴ he had no authorization to take this database from its owner and thus his taking it constituted stealing it.

The evidence showed that the valuation of the Net-Centric Diplomacy database was over \$4 million.¹³⁵

The evidence showed that 18 U.S.C. 641 exists and that PFC Manning's conduct in stealing the database and converting it to his own use and the use of WikiLeaks was prejudicial to good order and discipline and was service discrediting.

I thus conclude that reasonable grounds exist to believe that PFC Manning committed the offense alleged in Specification 12 of Additional Charge II.

Additional Charge II, Specification 13 (Art. 134, UCMJ; 18 U.S.C. 1030(a)(1)):

Lrw

In order to prove this offense, the government must establish the following six elements:

¹³⁰ PFC Manning's Secondary SIPRNET Computer Forensic Report, Bates # 00199494-507, at 1, 12-14.

¹³¹ PFC Manning's Personal Computer Forensic Report, Bates # 00124283-362, at 51-54.

¹³² DoS Files Forensic Report, Bates # 00054320-34, at 14.

¹³³ Lamo Chat, IO Ex. 19(D), at 33.

¹³⁴ Testimony of CPT Lim (stating he gave analysts the link through email to access diplomatic cables).

¹³⁵ NCD Valuation Documents. Bates # 00410556-60.

Continuation Sheet, DD Form 457, U.S. v. PFC Bradley E. Manning

- (1) that at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, the accused knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer;
- (2) that the accused obtained information that has been determined by the United States government by Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: more than seventy-five classified United States Department of State cables;
- (3) that the accused had reason to believe that the information he obtained could be used to the injury of the United States or to the advantage of any foreign nation;
- (4) that the accused willfully communicated, delivered, or transmitted the said information to a person not entitled to receive it;
- (5) that 18 U.S.C. section 1030(a)(1) exists; and
- (6) that, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.¹³⁶

Facts

The evidence showed that PFC Manning's primary SIPRNET computer contained, under his user profile, a file named "files.zip" in the "bloop" folder that had over 10,000 Department of State cables in .html web page format, and that over 4,000 of these cables were classified.¹³⁷ A CD accessed on PFC Manning's personal computer containing files.zip was burned on 4 May 10.¹³⁸ The evidence showed that another document in the "bloop" folder, "backup.xlsx," was a spreadsheet with cables published in March, April, and May 2010.¹³⁹ The tab in this spreadsheet including cables published in March and April 2010 started with a cable with number 251,288. The evidence showed that PFC Manning's primary SIPRNET computer had a version of wget (software used to download files from a server) that was the same version found in the Department of State log files, the Intelink log files, and that was downloaded on a NIPRNET computer by a user of PFC Manning's user profile.¹⁴⁰ A user of PFC Manning's user profile on that NIPRNET computer did Google searches for WikiLeaks and wget.exe on 3 May 10 and downloaded wget to that profile. A user of PFC Manning's user profile then transferred wget from the NIPRNET to SIPRNET on 4 May 2010, under PFC Manning's user profile.¹⁴¹

¹³⁶ These elements are a tailored version of Eighth Circuit Model Jury Instruction 6 18.103A.

¹³⁷ Testimony of SA Shaver. PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 31.

¹³⁸ Testimony of SA Shaver.

¹³⁹ PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 31; spreadsheet, at Bates # 00296982; Testimony of SA Shaver.

¹⁴⁰ PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 37

¹⁴¹ Testimony of SA Shaver.

The evidence showed that on 20 August 2011, WikiLeaks released 251,287 Department of State cables in unredacted form and made them available on the Internet.¹⁴² While the evidence was that WikiLeaks did not release the cables in the files.zip folder,¹⁴³ the forensic examination found thousands of State Department cables in unallocated space on PFC Manning's primary SIPRNET computer, ranging in classification from unclassified to secret; many were complete, but many others were not.¹⁴⁴ Additionally, the forensic examination of PFC Manning's primary SIPRNET computer revealed that a deleted and partially overwritten file named "c:\Lost File\backup\farah.zip" was originally created on 10 April 2010 and contained 582 Department of State Cables, over 250 of which were classified.¹⁴⁵ The evidence showed the Department of State cables were in .csv format, a way of moving files from one database to another, and were Base64 encoded.¹⁴⁶ Analysis of PFC Manning's secondary SIPRNET computer and his personal computer also showed many Department of State cables that had been converted to Base64 and stored in .csv format.¹⁴⁷ Specifically, approximately 113,000 complete Department of State cables converted to Base64 were found in a deleted .csv file in Unallocated Clusters on PFC Manning's secondary SIPRNET computer,¹⁴⁸ and evidence of Department of State cables published before March 2010 were found in Unallocated Clusters on PFC Manning's personal computer, including data appearing to have a .csv file structure listing Department of State cables with numbers preceding 251,287 in a format similar to the cables found on PFC Manning's primary SIPRNET Computer.¹⁴⁹ Additionally, examination of Department of State cable message record numbers released by WikiLeaks identified 251,298 individual message record numbers; examination of PFC Manning's personal computer and his primary and secondary SIPRNET computers showed that they contained 83% of all the message record numbers released to WikiLeaks.¹⁵⁰

This evidence, taken together, leads to a conclusion that the 251,287 files released by WikiLeaks were provided to WikiLeaks by PFC Manning.

The evidence showed that in his chats with Mr. Lamo concerning the State Department cables, PFC Manning said, "it was forwarded to WL ... and god knows what happens now ... hopefully worldwide discussion, debates, and reforms ... I want people to see the truth... regardless of who they are... because without information, you cannot make informed decisions as a public,"¹⁵¹ which indicates that that he had reason to believe that the information he obtained could be used to the injury of the United States or to the advantage of any foreign nation

¹⁴² Testimony of SA Bettencourt; Testimony of SA Shaver.

¹⁴³ Testimony of SA Shaver. SA Shaver also testified there was a problem with files.zip when it was created, and if a person using WinZip tried to open it, it would not open because it was a corrupted file, and one would need special tools to open the files in files.zip. Based on that testimony, it appears that WikiLeaks did not release the cables in files.zip because they could not open them.

¹⁴⁴ Testimony of SA Shaver.

¹⁴⁵ PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 34-36.

¹⁴⁶ Testimony of SA Shaver.

¹⁴⁷ PFC Manning's Primary SIPRNET Computer Forensic Report, Bates # 00211037-110, at 36.

¹⁴⁸ PFC Manning's Secondary SIPRNET Computer Forensic Report, Bates # 00199494-507, at 1, 12-14.

¹⁴⁹ PFC Manning's Personal Computer Forensic Report, Bates # 00124283-362, at 51-54.

¹⁵⁰ DoS Files Forensic Report, Bates # 00054320-34, at 14.

¹⁵¹ Lamo Chat, IO Ex. 19(D), at 33.

Continuation Sheet, DD Form 457, U.S. v. PFC Bradley E. Manning

While there was evidence that PFC Manning had the authority to access diplomatic cables for his job,¹⁵² the context of that evidence was that access was authorized for the analysts to do their job. The evidence also showed that before logging on to his primary and secondary SIPRNET computers, PFC Manning had to click "OK" on a warning banner, the first sentence of which read, "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only."¹⁵³ Accordingly, accessing diplomatic cables in order to provide them to a person not entitled to receive it exceeded authorized access. PFC Manning had no authorization to transfer this information to WikiLeaks, which was not entitled to receive it.

The evidence showed that these cables were properly classified and remain classified.¹⁵⁴

The evidence showed that 18 U.S.C. 1030(a)(1) exists and that PFC Manning's conduct in providing these classified cables to WikiLeaks was prejudicial to good order and discipline and was service discrediting.

Additional Charge II, Specification 14 (Art. 134, UCMJ; 18 U.S.C. 1030(a)(1)):

Law

In order to prove this offense, the government must establish the following six elements:

- (1) that at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 18 February 2010, the accused knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer;
- (2) that the accused obtained information that has been determined by the United States government by Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: a classified United States Department of State cable titled "Reykjavik-13";
- (3) that the accused had reason to believe that the information he obtained could be used to the injury of the United States or to the advantage of any foreign nation;
- (4) that the accused willfully communicated, delivered, or transmitted the said information to a person not entitled to receive it;
- (5) that 18 U.S.C. section 1030(a)(1) exists; and
- (6) that, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces.

¹⁵² Testimony of CPT Lim (stating he gave analysts the link through email to access diplomatic cables).

¹⁵³ Testimony of SA Shaver, IO Ex. 11(P), at 1 (Bates # 00376856).

¹⁵⁴ Classification Review, Bates # 00376903-53.

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

GOVERNMENT RESPONSE TO
DEFENSE REQUESTED
INSTRUCTION: SPECIFICATIONS
13 AND 14 OF CHARGE II

6 July 2012

RESPONSE

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny giving the Defense Requested Instruction for Specifications 13 and 14 of Charge II. The United States requests the Court consider its Response to the Renewed Defense Motion to Dismiss for Failure to State an Offense: Specifications 13 and 14 of Charge II for a more detailed response to the issues raised by the proposed defense instructions.

The United States objects to the defense instruction in its entirety, including any instructions that incorporate a mistake of fact defense before the presentation of evidence. The United States objects specifically to the following italicized portions:

Court Instructions

(1) That the accused did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, accessed a computer with authorization, but exceeded his authority in accessing the information in question on a Secret Internet Protocol Router network computer;

(2) That the accused knowingly exceeded his authorized access;

Comment: Misstates the elements. *See* Model Crim. Jury Instr. 9th Cir. 8.95 (2010) (Enclosure 5 to the Government's Proposed Member Instructions).

(3) That the accused, by means of such conduct, obtained information protected against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data to wit: more than 75 classified United States Department of State cables, with the intent to use such information against the interests of the United States;

Comment: Inaccurate statement of the law. The United States is not required to prove that the accused obtained information "with the intent to use such information against the interests of the United States." *See* S. Rep. No. 104-357, at 2, 13 (1996).

Court Definitions

(1) Exceeding Authorized Access to a Computer

The first element that the government must prove beyond a reasonable doubt is that the accused accessed a computer with authorization, but exceeded his authority in accessing the information in question.

In this case, the government charges that the accused, while authorized to access the computer, exceeded his authority in accessing the information in question. Under the statute, this requires that the government prove beyond a reasonable doubt that the accused had access to the computer, and used that access to obtain or alter information in the computer that the accused was not entitled to obtain or alter. In other words, the term 'exceeds authorized access' applies to 'inside hackers', individuals whose initial access to a computer is authorized but who access unauthorized information or files."

This element is not satisfied by mere misuse or misappropriation of information that the accused was authorized to access. Nor does it apply where the accused accesses information that he was authorized to access, but in an unauthorized manner. Rather, this element is only satisfied where the accused is authorized to access the computer and obtains or alters information on that computer that the accused is not entitled to obtain or alter.

If you find that the accused had authorization to access the computer and to obtain the information, you must find the accused not guilty.


Comment: This set of instructions raises issues related to the extent of the holding in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012), and the Government's theory that the accused "exceeded authorized access." The United States requests the Court consider its Response to the Renewed Defense Motion to Dismiss for Failure to State an Offense: Specifications 13 and 14 of Charge II as its objection to the above instruction is explained in detail.

(3) Obtaining Protected or Restricted Information

The third element that the government must prove beyond a reasonable doubt is that the accused obtained information protected against unauthorized disclosure for reasons of national defense or foreign relations or any restricted data, with the intent to use such information against the interests of the United States.

If you find that the information allegedly obtained by the accused was not protected against disclosure for reasons of national defense or foreign relations and was not restricted data, or that the accused did not have a reason to believe that the information could be used against the interests of the United States or to the advantage of a foreign nation, you must find the accused not guilty.

Comment: Inaccurate statement of the law. The language of the statute was amended in 1996 to track the scienter requirement in 18 U.S.C. § 793(e). The United States is not required to prove that the accused obtained information "with the intent to use such information against the interests of the United States." See S. Rep. No. 104-357, at 2, 13 (1996). Additionally, the standard is not whether the accused had reason to believe that the information could be "used against the interests of the United States...."


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 6 July 2012.


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

GOVERNMENT RESPONSE TO
DEFENSE REQUESTED
INSTRUCTION: SPECIFICATION
1 OF CHARGE II

6 July 2012

RESPONSE

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny giving the Defense Requested Instruction for Specification 1 of Charge II. The proposed defense instructions are confusing and incomplete in that they do not define necessary terms and phrases.

The United States objects to the defense instruction in its entirety, including any instructions that incorporate a mistake of fact defense before the presentation of evidence. The United States objects specifically to the following italicized portions:

Court Definitions

"Wanton" or "wantonly" includes "recklessness" but may connote willfulness, or a disregard of probable consequences, and thus describes a more aggravated offense.


Comment: The United States maintains that "wantonly" does not necessarily describe a more aggravated offense than "recklessness." See Government's Proposed Member Instructions, at 4.

A person causes intelligence to be published on the Internet when the person personally publishes the intelligence on the Internet or knowingly or intentionally induces or sets in motion acts by an animate or inanimate agency or instrumentality which result in the publication of the intelligence on the Internet.

Comment: This instruction will confuse the fact finder. There is no requirement that the act be carried out "knowingly or intentionally." The act must be done wrongfully and wantonly. See Charge Sheet.

Maximum Punishment

Comment: The Government opposes the characterization of this offense as a violation of Article 92. The Court has already ruled that Specification 1 of Charge II encompasses more information than AR 380-5. See Appellate Exhibit LXXX. It includes additional elements, such as knowledge that the intelligence would be accessible to the enemy, which is an aggravator. The offense is more closely-related to a violation of 18 U.S.C. § 793(e), which carries a maximum penalty of ten years confinement.


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 6 July 2012.


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

GOVERNMENT RESPONSE TO
DEFENSE REQUESTED
INSTRUCTION: SPECIFICATIONS
2, 3, 5, 7, 9, 10, 11, AND 15
OF CHARGE II

6 July 2012

RESPONSE

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny giving the Defense Requested Instruction for Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II.

The United States objects to the defense instruction in its entirety, including any instructions that incorporate a mistake of fact defense before the presentation of evidence. The United States objects specifically to the following italicized portions:

Court Instructions

In Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II, the accused is charged with the offense of Espionage, a violation of 18 U.S.C. Section 793(e). To find the accused guilty of this offense with regards to Specification 2, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following five (5) elements:

Comment: The accused is not charged with Espionage. The accused is charged with Transmitting National Defense Information under 18 U.S.C. § 793(e).

Possession

A person has "unauthorized" possession of something if he is not entitled to have it.

Comment: This instruction will confuse the fact finder. The accused was an all-source intelligence analyst for the Army and had access to the national defense information at issue. An individual has unauthorized possession of information if they possess the information in a location which is contrary to law or regulation for the conditions of their employment. See Enclosure 1 to the Government's Proposed Member Instructions.

Information Related to the National Defense

However, only information of the type which, if disclosed, could threaten the national security of the United States meets the definition of information "related to the national defense" for the purpose of this section. The connection must not be a strained one or an arbitrary one. The relationship must be reasonable and direct. Further, the type of harm that disclosure of the information is likely to cause must be endangerment to the environment of physical security

which a functioning democracy requires. Finally, the Government must prove beyond a reasonable doubt that disclosure of the information would be likely to cause imminent serious injury to the United States. If the disclosure of this information does not pose this threat of imminent serious injury to the United States, then it is not information relating to the national defense.

Comment: To the Government's knowledge, this instruction has never been given in a prosecution under § 793. The instruction is an inaccurate characterization of the law. The language, in part, appears to have been drawn from dicta in the concurring opinion of Judge Wilkinson in *United States v. Morison*, 844 F.2d 1057, 1082 (4th Cir. 1988). Some of the language ("imminent serious injury") appears to have been drawn from dicta in *New York Times Co. v. United States*, 403 U.S. 713, 726-27 (1971), an unrelated case that considered the Government's attempt to prevent press entities from publishing the "Pentagon Papers."


Additionally, the Government must prove beyond a reasonable doubt that the Government closely held the information and that the accused knew the information was closely held. To do this, the Government must prove at least two things: (1) that the information was classified and (2) that the information was not otherwise available to the public. If, however, the information is lawfully accessible to anyone willing to take pains to find, to sift, and to collate it, you may not find the accused guilty of espionage under this section. Only information relating to our national defense which is not available to the public at the time of the claimed violation falls within the prohibition of this section.

Comment: To the Government's knowledge, this instruction has never been given in a prosecution under § 793. The instruction is also an inaccurate statement of the law. See Enclosure 1 to the Government's Proposed Member Instructions; *Morison*, 844 F.2d at 1071-72. The United States is not required to prove that information is classified in order to prove that the information was closely held, and thus related to the national defense. The fact that national defense information is classified is probative of whether that information was closely held. See Enclosure 1 to the Government's Proposed Member Instructions.


Information could be used to injury of the United States

Additionally, the likelihood of the information being used to the injury of the United States or to the advantage of any foreign nation must not be too remote, hypothetical, speculative, far-fetched or fanciful. Rather, the information must pose a legitimate danger of being used to the injury of the United States or to the advantage of any foreign nation, such that an accused knew or should have known about the information's capability to be used in this manner.

Comment: To the Government's knowledge, this instruction has never been given in a prosecution under § 793 and is not consistent with the law, as drafted. Section 793 requires the United States to prove the accused knew or should have known the information "could be used to the injury of the United States or to the advantage of any foreign nation" and does not require the United States to prove that the information poses a "legitimate danger of being used..." Further, there is no requirement that the United States prove the accused knew or should have known of "the information's capability to be used in this manner."


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 6 July 2012.


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211)

Prosecution Supplemental Response
to Defense Motion to Compel Discovery #2

9 July 2012

RELIEF SOUGHT

The prosecution respectfully requests the Court deny, in part, the Defense Addendum to Defense Motion to Compel Discovery #2 (hereinafter "Defense Motion") insofar as the defense's request consists of the following three categories of information that are not relevant and necessary for production under RCM 703:

(1) Information that predated, and contributed to, the Department of State (the "Department") draft damage assessment dated August 2011;

(2) Purely administrative records; and

(3) Personally Identifiable Information (PII) of persons negatively affected by the unauthorized disclosures, to include those persons identified by the WikiLeaks Persons at Risk Group (WPAR) as being put at risk.

This Supplemental Response also serves as notice to the Court for which of the requested records exist.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the defense bears the burden of persuasion and must prove any factual issues necessary to decide this motion by a preponderance of the evidence. See Manual for Courts-Martial, United States, RCM 905(c) (2012).

FACTS

On 18 May 2012, the prosecution made the Department's draft damage assessment dated August 2011 available to the defense for inspection.

On 7 June 2012, three Department witnesses, specifically Ms. Marguerite Coffey, Ms. Rena Bitter, and Ms. Catherine Brown, testified during a motions hearing in the above captioned courts-martial. The witnesses referenced the below records in their testimony and testified that they were unaware whether the below records remain in existence:

(1) Written assessments produced by the Chiefs of Mission used to formulate a portion of the draft damage assessment completed in August of 2011;

APPELLATE LAWSUIT 192
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

(2) Written Situational Reports produced by the WikiLeaks Working Group between roughly 28 November 2010 and 17 December 2010;

(3) Written minutes and agendas of meetings by the Mitigation Team;

(4) Information Memorandum for the Secretary of State produced by the WPAR;

(5) A matrix produced by WPAR to track identified individuals;

(6) Formal guidance produced by WPAR and provided to all embassies, including authorized actions for any identified person at risk;

(7) Information collected by the Director of the Office of Counter Intelligence and Consular Support within the Department of State regarding any possible impact from the disclosure of diplomatic cables;¹ and

(8) Any prepared written statements for the Department's reporting to Congress on 7 and 9 December 2010.

See Appellate Exhibit (AE) CXXXXII.

On 7 June 2012, the prosecution requested the Court delay the Court's ruling on the Defense Motion to Compel Discovery #2 for information pertaining to the Department for thirty days to search for the above referenced records. See id.

On 7 June 2012, the defense submitted its Addendum to Defense Motion to Compel Discovery #2 and requested the above records. The defense requested that the prosecution disclose this material under RCM 701(a)(2) or, in the alternative, RCM 703.² The defense also requested that the prosecution disclose this material under RCM 701(a)(6). See id.

On 8 June 2012, the Court ordered the prosecution to immediately begin the process of searching for and inspecting the above records. The Court ordered the prosecution to notify the Court no later than 9 July 2012 which of the above records exist and, for those records that do exist, file a supplemental response to the Defense's Motion to Compel Discovery #2. See id.; see also AE CXLVII at 7.

The Department searched for the above records and information and made all found material available at the Department for review by the prosecution. The prosecution reviewed all the provided material (except where otherwise annotated below) at the Department and hereby notifies the Court of its findings:

¹ The job title of the individual is the Director of the Office of Counter Intelligence and Consular Support within the Bureau of Intelligence and Research, not the Director of the Office of Counterintelligence.

² On 22 June 2012, the Court ruled that "[e]vidence maintained by other government agencies, whether aligned with the Prosecution or not, are not within the control of military authorities IAW RCM 701(a)(2)." AE CXLVII at 5.

(1) The written assessments produced by the Chiefs of Mission used to formulate a portion of the draft damage assessment completed in August of 2011 consist largely of cables sent to, and from, affected embassies relating to the cables released up until August of 2011;

(2) The written Situational Reports produced by the WikiLeaks Working Group, a 24/7 working group composed of senior officials from throughout the Department designed to monitor the immediate crisis stemming from the released cables and coordinate the Department's response, between roughly 28 November 2010 and 17 December 2010, consist of the then real-time developments regarding cables released up until that time, summaries of published news articles relating to the cables released up until that time, and updates from select regions of the world regarding the cables released up until that time;

(3) The written minutes and agendas of meetings by the Mitigation Team, a group created to address the policy, legal, security, counterintelligence, and information assurance issues presented by the release of these documents, consist of formal meeting notes, PowerPoint slides of administrative matters and substantive issues, and documentation on information exchanged with other federal organizations;

(4) The Information Memoranda for the Secretary of State produced by WPAR, a group tasked with identifying persons referenced in released cables who are at risk, providing guidance to local embassies who request assistance on behalf of those persons, and tracking all persons at risk, consist of background information relating to the creation of the WPAR, any assistance requested by embassies from the WPAR (to include examples of requested assistance), regional reports by bureaus, guidance to embassies on how to identify and assist persons at risk, summaries of WPAR's duties, and the status of reviewed cables related to persons at risk;

(5) The matrices produced by WPAR consist of PII of individuals and their family members who are identified by WPAR as persons at risk based on the released cables to track the status of these individuals;³

(6) The formal guidance produced by WPAR and provided to all embassies, including authorized actions for any identified person at risk consists of procedures for embassies seeking assistance from WPAR, the steps the Department takes should someone request relocation, additional options available to the embassies, and a list of best practices;

(7) The information collected by the Director of the Office of Counter Intelligence and Consular Support within the Department regarding any possible impact from the disclosure of diplomatic cables consists of translated foreign open-source internet articles, select cables, the Department's draft damage assessment dated August 2011 to which the defense already has access, regional assessments relating to the released cables, and no other versions of the draft assessment;⁴ and

³ For the purpose of this Motion, the prosecution considers PII to include any information that could be used by another to identify a specific individual.

(8) The Department did not find any prepared written statements for the Department's reporting to Congress on 7 and 9 December 2010. Based on those dates and Under Secretary Kennedy's testimony, only informal discussions would have occurred between Department officials and members of Congress, therefore there are no written statements or other documents.

WITNESSES/EVIDENCE

The prosecution does not request any witnesses or evidence be produced for this response. The prosecution respectfully requests that the Court consider the Appellate Exhibits referenced herein.

LEGAL AUTHORITY AND ARGUMENT

The Due Process Clause of the Fifth Amendment requires the prosecution to disclose evidence that is favorable to the defense and material to guilt or punishment. See Brady v. Maryland, 373 U.S. 83 (1963). RCM 701(a)(6) states that the prosecution "shall, as soon as practicable, disclose to the defense the existence of evidence known to the trial counsel which reasonably tends to negate the guilt of the accused of an offense charged, reduce the degree of guilt of the accused of an offense charged, or reduce the punishment." RCM 701(a)(6). The prosecution will disclose to the defense, or submit to the Court for *in camera* review for limited disclosure under MRE 505(g)(2), any records found that are discoverable under Brady or RCM 701(a)(6), for which the a privilege under MRE 505(c) is not claimed.

RCM 703(f) states that "[e]ach party is entitled to the production of evidence which is relevant and necessary." RCM 703(f)(1); see also United States v. Graner, 69 M.J. 104, 107 (C.A.A.F. 2010) (stating that RCM 703 is "grounded on the fundamental concept of relevance"); MRE 401 (defining relevant evidence as "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence"). The discussion to the rule states that "[r]elevant evidence is necessary when it is not cumulative and when it would contribute to a party's presentation of the case in some positive way on a matter in issue." RCM 703(f)(1), discussion. Evidence that is material to the preparation of the defense under the control of other government agencies can be relevant and necessary for discovery, requiring production of the evidence under RCM 703. See AE CXLVII at 5. The burden is on the defense for production of evidence outside the control of military authorities for discovery under the relevant and necessary standard in RCM 703. See RCM 905(c); see also AE CXLVII at 5.

For the reasons below, the following information within the above categories are not relevant and necessary for production under RCM 703: (1) information that predated, and contributed to, the Department's draft damage assessment dated August 2011; (2) purely administrative records; and (3) PII of persons negatively affected by the unauthorized disclosures, to include those persons identified by WPAR as being put at risk.

⁴ The prosecution did not finish its review of all the cables in this category based on the volume of information. The prosecution estimates that it has approximately 500 more cables to review.

- I: ABSENT THAT WHICH IS DISCOVERABLE UNDER BRADY OR RCM 701(a)(6), INFORMATION THAT PREDATED, AND CONTRIBUTED TO, THE DEPARTMENT'S DRAFT DAMAGE ASSESSMENT IS NOT NECESSARY BECAUSE IT IS CUMULATIVE TO THE DEPARTMENT'S DRAFT DAMAGE ASSESSMENT WHICH THE PROSECUTION HAS MADE AVAILABLE TO THE DEFENSE FOR INSPECTION.

"Relevant evidence is necessary when it is not cumulative and when it would contribute to a party's presentation of the case in some positive way on a matter in issue." RCM 703(f)(1), discussion. On 18 May 2012 and based on the Court's ruling, the prosecution made the Department's draft damage assessment available to the defense for inspection. Absent that which is discoverable under Brady or RCM 701(a)(6), information that predated, and contributed to, the Department's draft damage assessment is cumulative, thus not subject to production under RCM 703.

The following categories contain information that predated, and likely contributed to, the Department's draft damage assessment, and therefore are cumulative:

- (1) Written assessments produced by the Chiefs of Mission used to formulate a portion of the draft damage assessment completed in August of 2011;
- (2) Written Situational Reports produced by the WikiLeaks Working Group between roughly 28 November 2010 and 17 December 2010;
- (3) Written minutes and agendas of meetings by the Mitigation Team;
- (4) Information Memorandum for the Secretary of State produced by WPAR;
- (5) Matrices produced by WPAR to track identified individuals; and
- (6) Formal guidance produced by WPAR and provided to all embassies, including authorized actions for any identified person at risk.

- II: PURELY ADMINISTRATIVE RECORDS ARE NOT RELEVANT AND NECESSARY.

Relevant evidence "means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." RCM 401; see also Graner, 69 M.J. at 108 (RCM 703 is "grounded on the fundamental concept of relevance"). "Relevant evidence is necessary when it is not cumulative and when it would contribute to a party's presentation of the case in some positive way on a matter in issue." RCM 703(f)(1), discussion.

A portion of the written minutes and agendas of meetings by the Mitigation Team contain purely administrative records without any substantive value or that have no identifiable connection with the relevant mitigation effort. Such records are irrelevant and would not

"contribute to a party's presentation of the case in some positive way," thus not subject to production under RCM 703.

- III: PERSONALLY IDENTIFIABLE INFORMATION OF PERSONS NEGATIVELY AFFECTED BY THE ACCUSED'S CHARGED MISCONDUCT, SPECIFICALLY ANY SUCH INFORMATION LISTED ON THE MATRICES PRODUCED BY THE WIKILEAKS PERSONS AT RISK GROUP, IS NOT DISCOVERABLE OR RELEVANT AND NECESSARY FOR PRODUCTION.

PII of persons negatively affected by the accused's charged misconduct, particularly those persons put at risk based on the released Department cables, is not discoverable under Brady or RCM 701(a)(6). Further, such information is not relevant and necessary under RCM 703 because such information, *inter alia*, would not "contribute to a party's presentation of the case in some positive way on a matter in issue." Even if material to the preparation of the defense, any PII of persons put at risk based on the released Department cables is not material to the preparation of the defense to the extent that it is relevant and necessary.

- IV: SHOULD THE COURT ORDER THE PRODUCTION OF THE ABOVE RECORDS, THE PROSECUTION REQUESTS NO LESS THAN 45-60 DAYS TO NOTIFY THE COURT WHETHER THE PROSECUTION WILL SEEK LIMITED DISCLOSURE IAW MRE 505(g)(2) OR CLAIM A PRIVILEGE ON BEHALF OF THE DEPARTMENT IAW MRE 505(c) AND TO PRODUCE THE RECORDS TO THE DEFENSE, IF NECESSARY.

Assuming, *arguendo*, the Court orders production of the above records or some portion thereof, the prosecution requests no less than 45-60 days to notify the Court whether the Department will seek limited disclosure under MRE 505(g)(2) or claim a privilege under MRE 505(c) and to produce the documents under RCM 701(g), MRE 505(g)(2), or MRE 505(c), if necessary. Based on the prosecution's review, the prosecution estimates that the above records total more than 5,000 documents, a large majority of which are marked classified. The prosecution estimates that the Department will need no less than 45-60 days to review those documents for which production is ordered to determine whether it will seek limited disclosure or claim a privilege.

CONCLUSION

For the above reasons, the prosecution respectfully requests the Court deny, in part, the Defense Motion insofar as the defense's request consists of the following three categories of information that are not relevant and necessary for production under RCM 703:

(1) Information that predated, and contributed to, the Department's draft damage assessment dated August 2011;

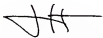
(2) Purely administrative records; and

(3) PII of persons negatively affected by the unauthorized disclosures, to include those persons identified by WPAR as being put at risk.



J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel, via electronic mail, on 9 July 2012.



J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

theguardian

AP review finds no WikiLeaks sources threatened

- AP foreign, Saturday September 10 2011

CASSANDRA VINOGRAD

Associated Press= WASHINGTON (AP) — Federica Ferrari Bravo's story of meeting American diplomats in Rome seven years ago hardly reads like a James Bond spy novel or a Cold War tale of a brave informant sharing secrets to help the United States.

So it came as a something of a surprise to her to hear that in one of the 250,000-odd State Department cables released by the anti-secrecy website WikiLeaks, she was deemed a source so sensitive U.S. officials were advised not to repeat her name.

"I don't think I said anything that would put me at risk," the Italian diplomat said.

There are similar stories involving other foreign lawmakers, diplomats and activists cited in the U.S. cables as sources to "strictly protect."

An Associated Press review of those sources raises doubts about the scope of the danger posed by WikiLeaks' disclosures and the Obama administration's angry claims, going back more than a year, that the revelations are life-threatening. U.S. examples have been strictly theoretical.

The question of whether the dire warnings are warranted or overblown became more acute with the recent release all of the 251,287 diplomatic memos WikiLeaks held.

Tens of thousands of confidential exchanges were dumped, emptying a trove of documents. They were released piecemeal since last year, initially with the cooperation of a select group of newspapers and magazines that blacked out some names and information before publishing the documents.

The latest cables were published in full, without names blacked out. State Department spokeswoman Victoria Nuland branded the action "irresponsible, reckless and frankly dangerous," and the U.S. said the release exposed the names of hundreds of sensitive sources.

WikiLeaks founder Julian Assange has blamed Britain's Guardian newspaper for publishing a secret encryption code, allowing intelligence agencies to access the cables and forcing WikiLeaks to provide the people affected the same information.

But the AP's review of the sources found several of them comfortable with their names in the open and no one fearing death. Others are dead, their names cited as sensitive in the context of long-resolved

APPELLATE EXHIBIT *CXCW*
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

Enclosure 1

(192)

conflicts or situations. Some have written or testified at hearings about the supposedly confidential information they provided the U.S. government.

The AP survey is selective and incomplete; it focused on those sources the State Department seemed to categorize as most risky.

The AP did not attempt to contact every named source in the new trove. It's generally up to the embassies themselves to decide which identities require heightened vigilance, officials say.

Hadzira Hamzic, a 73-year-old Bosnian refugee, wasn't bothered about being identified as one of thousands of victims from the Balkan wars of the 1990s.

"I never hid that," she told the AP. "It is always hard when I have to tell about how I had been raped, but that is part of what happened and I have to talk about it."

In Asia, former Malaysian diplomat Shazryl Eskay Abdullah was shocked that an "unofficial lunch meeting" he had several years ago with a U.S. official meant his name ended up on a formal report. But he said his role in southern Thailand peace talks was well known. "I don't see why anyone would come after me," Shazryl said.

Ferrari Bravo's subject matter was also by no means mundane. A veteran of her nation's embassy in Tehran, Ferrari Bravo worked at the time on the Italian Foreign Ministry's Iran desk and discussed with the U.S. her government's view of the Iranian nuclear standoff. She urged continued dialogue.

"There is nothing that we said that was not known to our bosses, to our ministers, to our heads of state," she said. On having her identity protected, she said: "We didn't ask. There is nothing to protect."

U.S. officials say they have two criteria for sensitive sources. The first deals with people in totalitarian societies or failed states who could be imprisoned or killed, or perhaps denied housing, schooling, food or other services if exposed as having helped the United States.

The State Department also has sought to censor names of people who might lose their jobs or suffer major embarrassment even in friendly countries, if they were seen offering the U.S. candid insights or restricted information.

One such case involved the dismissal in December of a top aide to German Foreign Minister Guido Westerwelle after he provided details on coalition talks and debates over issues such as U.S. nuclear weapons in Europe.

Still, the total damage appears limited and the State Department has steadfastly refused to describe any situation in which they've felt a source's life was in danger. They say a handful of people had to be relocated away from danger but won't provide any details on those few cases.

Units throughout the department have been scouring the documents since last year to find examples where sources are exposed and inform them that they may be "outed." Some, such as Hamzic, Sharzyl and Ferrari Bravo, say they were never contacted. Presumably, endangered individuals would have been prioritized.

Clearly, sensitivities depend on context. Revelations that may cause personal or political discomfort for a U.S. embassy contact in Western Europe may be life-threatening for an informant in an undemocratic nation. In the cables, they may both be "strictly protected" sources, highlighting relative danger levels in different places.

In Vietnam, the U.S. seemed to be dealing with sources whose names demanded vigilance: the wife of a dissident sentenced to five years in prison; a Buddhist leader condemning the arrest of a fellow priest; a dissident who says people "held his family hostage" until he renounced his activism; a Christian preacher complaining of police pressure on him to renounce his faith; another who speaks of a colleague forcibly sent to a mental institute.

A Syrian human rights activist warned the U.S. of a looming crackdown on anti-government activists as far back as 2009. If the activist wasn't threatened by the disclosure last year, he may be now that the country is in the throes of a brutal five-month security operation.

In Mexico, the term "strictly protect" appeared to be attached to interlocutors indiscriminately, even when officials offered only flattering assessments of their government or said little that wasn't common knowledge. It perhaps makes more sense in the context of a country where organized crime networks have essentially fought an insurgency against the government, where allowing a valued source's name to get out could affect that person's safety.

Assange, an Australian, has defended his actions by saying no one has died as a result of WikiLeaks.

Current and former American officials say that argument misses the point.

Making people think twice before providing the U.S. with information — or simply refuse ever again to help — hurts the good causes of human rights and democracy that American officials are promoting, they argue.

Take Arnold Sundquist, a Swede whose life isn't in danger. He provided the U.S. Embassy with sensitive details on an Iranian attempt to buy helicopters and said he was unhappy that his actions were now public. Last year, Swedish media with access to the WikiLeaks trove reported on the incident but didn't mention him by name.

"It is what it is," he said. "I can't do anything about it."

But will he or others in a similar situation, be as ready to help American authorities again?

Venezuelan journalist Nelson Bocaranda thinks not. His identity was exposed in a document describing how he told the U.S. ambassador in 2009 that according to one of his sources, Colombian rebel leaders had visited Caracas for secret meetings with senior Venezuelan government officials. Bocaranda published the account in one of his newspaper columns.

"I feel betrayed by WikiLeaks," Bocaranda told the AP on Friday. But he said that as a journalist it's natural for him to talk with diplomats from various countries. "I think the ones who have been betrayed basically are the American diplomats," he said.

"It's going to be more difficult for them because I think no one is going to want to talk for fear of coming out in print with their name," he said, adding that would apply those who might otherwise supply sensitive information.

He said he doesn't feel his work or personal security face additional threats as a result of his name being exposed but said he suspects President Hugo Chavez's government could try to "cast doubts on me, to say that I am a member of the CIA."

Bocaranda said that he has nothing to hide and that the information he publishes in his newspaper columns and on the Internet is public. "I don't think my sources are going to shut me out," he said.

Other governments have echoed the U.S. criticism of WikiLeaks, saying it jeopardizes invaluable diplomacy — the exchanges that aim to promote understanding, avoid war and improve global security.

The anger from Assange's home nation, Australia, was prompted not by the release of sources, but of 23 Australians who had been in contact with a Yemen-based al-Qaida offshoot and were being monitored. Still, a government statement couldn't point to a direct threat from the disclosure, only a potential danger.

"The large-scale distribution of hundreds of thousands of classified United States government documents is reckless, irresponsible and potentially dangerous," Australian Attorney-General Robert McClelland said.

Vinograd reported from London. Associated Press writers Nicole Winfield in Rome; Sean Yoong in Kuala Lumpur, Malaysia; Sabina Niksic in Sarajevo, Bosnia; Ian James in Venezuela; and Karl Ritter in Stockholm contributed to this report.

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**Prosecution Proposed
Case Calendar
Update**

29 June 2012

1. The Court is currently scheduling Article 39(a) sessions with the following default schedule at the request of the parties: two weeks for parties to file motions; two weeks for parties to file responses; five days for parties to file replies; and one week for the Court to review all pleadings before the start of the motions hearing. The time for filing replies was added after the first Article 39(a) session on 15-16 March 2012 because the Court received reply briefs the day before that session, the parties desire to continue to file replies, and the Court requires time to consider them.
2. The Prosecution Proposed Case Calendar Update, dated 29 June 2012, is based upon the same assumptions listed in the Prosecution Proposed Case Calendar (AE I) and all Prosecution Proposed Case Calendar Updates and Supplements (including AE XX, XLV, XLVI, CXIII, CLI, and the Prosecution Proposed Case Calendar Update, dated 22 June 2012). To the extent these assumptions prove to be incorrect or too ambitious, the schedule will be correspondingly longer.
3. Scheduling dates and suspense dates are set forth below. The trial schedule will be reviewed and updated as necessary at each scheduled Article 39(a) session.

- a. **Immediate Action (21 February 2012 - 16 March 2012)**
- b. **Legal Motions, excluding Evidentiary Issues (29 March 2012 - 26 April 2012)**
- c. **Legal Motions (10 May 2012 - 8 June 2012)**
- d. **Interim Pretrial Motions (2 June 2012 – 25 June 2012)**
- e. **Pretrial Motions (7 June 2012 – 20 July 2012)**
 - (A) Filing: 22 June 2012
 - (B) Response: 6 July 2012
 - (C) Reply: 11 July 2012
 - (D) Article 39(a): 16-20 July 2012

(1) Defense Motion to Compel Discovery #2 (Department of State Material)¹

- (A) Filing: 7 June 2012

¹ See Appellate Exhibit (AE) CXLII. AE CXLVII changed the response date to 9 July 2012.

- (B) Response: 9 July 2012
- (C) Reply: 11 July 2012
- (D) Article 39(a): 16-20 July 2012

(2) Government Initial Witness List

- (A) Filing: 22 June 2012

(3) Proposed Members Instructions for All Charged Offenses

(4) Witness Lists for Article 13

- (A) Defense Witness Lists: 3 July 2012²
- (B) Government Objections (if any): 10 July 2012
- (C) Defense Motion to Compel (if any): 13 July 2012
- (D) Article 39(a): 16-20 July 2012

(5) Preliminary Determinations on Admissibility

(6) Defense Motion to Dismiss All Charged Offenses under 18 U.S.C. 1030(a)(1) #2

(7) Maximum Punishment for Lesser Included Offenses

(8) Government Motion for Substitutions under MRE 505(g)(2) for FBI Impact Statement

(9) Government Motion for Modification of Court Order: Government Motion: Protective Order(s) dated 24 April 2012

(10) Supplemental Filings on Actual Damage on the Merits

- (A) Filings: 21 June 2012

(11) Proposed Questionnaires

- (A) Defense Filing: 6 July 2012
- (B) Prosecution Response: 11 July 2012
- (B) Article 39(a): 16-20 July 2012³
- (C) Questionnaires to Detailed Members and Alternates: 24 July 2012
- (D) Suspense for Detailed Members and Alternates to Respond: 3 August 2012

(12) Updated Proposed Case Calendar⁴

- (A) Filing: N/A

² The United States moved the date from 6 July 2012 to 3 July 2012 to allow more than one day to contact the witnesses after the defense provides a synopsis of the expected testimony sufficient to show its relevance and necessity.

³ Any disagreements between the parties' questionnaires will be resolved at the 16-20 July 2012 Article 39(a).

⁴ The parties will be ready to discuss the case calendar at the 27-31 August 2012 Article 39(a) session.

(B) Article 39(a): 27-31 August 2012

f. Interim Pretrial Motions (10 August 2012 @ 1300)

g. Pretrial Motions (20 July 2012 – 31 August 2012)

- (A) Filing: 3 August 2012
- (B) Response: 17 August 2012
- (C) Reply: 22 August 2012
- (D) Article 39(a): 27-31 August 2012

(1) Article 13

- (A) Filing: 27 July 2012⁵

(2) Motions in Limine

(3) Motions to Suppress (if any)

(4) Defense Notice of Intent to Disclose Classified Information under MRE 505(h)(1)

(5) Notification to the Court of Anticipated Limited Disclosures under MRE 505(g)(2) or Notification to the Court of Privilege under MRE 505(c) for Files under the Possession Custody, or Control of Military Authorities based on the Court's 22 June 2012 Ruling

- (A) Filing: 20 July 2012

(6) Notification to the Court of Anticipated Limited Disclosures under MRE 505(g)(2) or Notification to the Court of Privilege under MRE 505(c) for FBI Investigative File or Impact Statement based on the Court's 22 June 2012 Ruling

- (A) Filing: 25 July 2012

(7) Government Filing for *In Camera* Proceeding 1AW MRE 505(i) with Notice to Defense (if Privilege is Claimed) based on the Court's 22 June 2012 Ruling

- (A) Filing: 25 July 2012

(8) Disclosure to Defense or Disclosure to the Court under RCM 701(g)(2) or MRE 505(g)(2) of All Information Subject to the Court's 22 June 2012 Ruling⁶

- (A) Filing: 3 August 2012

⁵ The defense agreed to the filing date of one week earlier to give the United States the necessary time to respond.

⁶ This disclosure includes all files that involve investigation, damage assessment, or military measures that are under the possession, custody, or control of military authorities; all FBI files that involve investigation, damage assessment, or mitigation measures; the ODN/ONCIX damage assessment; and evidence the United States will introduce on the merits and during sentencing.

(9) Disclosure of All Remaining Unclassified or Classified (under MRE 505(g)(1)) Brady Material and Disclosure under MRE 701(g)(2) or MRE 505(g)(2) of All Remaining Classified Brady Material⁷

(A) Filing: 3 August 2012

(10) Witness Lists for Speedy Trial, including Article 10

(A) Witness Lists: 10 August 2012

(B) Government Objections (if any): 17 August 2012⁸

(C) Defense Motion to Compel (if any): 22 August 2012

(D) Article 39(a): 27-31 August 2012

(11) Updated Proposed Case Calendar⁹

(A) Filing: N/A

(B) Article 39(a): 27-31 August 2012

h. Interim Pretrial Motions (19 September 2012)

i. Pretrial Motions (7 September 2012 – 12 October 2012)

(A) Filing: 14 September 2012

(B) Response: 28 September 2012

(C) Article 39(a): 15-19 October 2012

(1) Speedy Trial, including Article 10

(A) Filing: 7 September 2012¹⁰

(2) Witness List (Defense and Supplemental Government)

(A) Filing: 14 September 2012

(B) Government Objection to Defense Witnesses: 21 September 2012

(C) Motion to Compel Production: 28 September 2012

(D) Response: 3 October 2012

(E) Article 39(a): 15-19 October 2012

(3) Defense Notice of its Intent to Offer the Defense of Alibi, Innocent Ingestion, or Lack of Mental Responsibility IAW RCM 701(b)(2)

⁷ This production includes any material discovered while searching the files, if any, of the President's Intelligence Advisory Board, and all material that is not subject to Motions to Compel Discovery or Production. If the Court rules that any of the proposed summaries under MRE 505(g)(2) are not acceptable, the prosecution will need additional time to obtain approval for a different substitution.

⁸ The Court and the parties discussed an objection date of 22 August 2012 in the 25 June 2012 RCM 802 Conference; however, the United States set the date earlier to allow the defense the opportunity to file a motion to compel, if necessary.

⁹ The parties will be ready to discuss the case calendar at the 27-31 August 2012 Article 39(a) session.

¹⁰ The defense agreed to the filing date of one week earlier to give the United States the necessary time to respond.

INSTRUCTIONS FOR PREPARING AND ARRANGING RECORD OF TRIAL

USE OF FORM - Use this form and MCM, 1984, Appendix 14, will be used by the trial counsel and the reporter as a guide to the preparation of the record of trial in general and special court-martial cases in which a verbatim record is prepared. Air Force uses this form and departmental instructions as a guide to the preparation of the record of trial in general and special court-martial cases in which a summarized record is authorized.

Army and Navy use DD Form 491 for records of trial in general and special court-martial cases in which a summarized record is authorized. Inapplicable words of the printed text will be deleted.

COPIES - See MCM, 1984, RCM 1103(g). The convening authority may direct the preparation of additional copies.

ARRANGEMENT - When forwarded to the appropriate Judge Advocate General or for judge advocate review pursuant to Article 64(a), the record will be arranged and bound with allied papers in the sequence indicated below. Trial counsel is responsible for arranging the record as indicated, except that items 6, 7, and 15e will be inserted by the convening or reviewing authority, as appropriate, and items 10 and 14 will be inserted by either trial counsel or the convening or reviewing authority, whichever has custody of them.

1. Front cover and inside front cover (chronology sheet) of DD Form 490.
2. Judge advocate's review pursuant to Article 64(a), if any.
3. Request of accused for appellate defense counsel, or waiver/withdrawal of appellate rights, if applicable.
4. Briefs of counsel submitted after trial, if any (Article 38(c)).
5. DD Form 494, "Court-Martial Data Sheet."
6. Court-martial orders promulgating the result of trial as to each accused, in 10 copies when the record is verbatim and in 4 copies when it is summarized.
7. When required, signed recommendation of staff judge advocate or legal officer, in duplicate, together with all clemency papers, including clemency recommendations by court members.

8. Matters submitted by the accused pursuant to Article 60 (MCM, 1984, RCM 1105).

9. DD Form 458, "Charge Sheet" (unless included at the point of arraignment in the record).

10. Congressional inquiries and replies, if any.

11. DD Form 457, "Investigating Officer's Report," pursuant to Article 32, if such investigation was conducted, followed by any other papers which accompanied the charges when referred for trial, unless included in the record of trial proper.

12. Advice of staff judge advocate or legal officer, when prepared pursuant to Article 34 or otherwise.

13. Requests by counsel and action of the convening authority taken thereon (e.g., requests concerning delay, witnesses and depositions).

14. Records of former trials.

15. Record of trial in the following order:

- a. Errata sheet, if any.
- b. Index sheet with reverse side containing receipt of accused or defense counsel for copy of record or certificate in lieu of receipt.
- c. Record of proceedings in court, including Article 39(a) sessions, if any.
- d. Authentication sheet, followed by certificate of correction, if any.
- e. Action of convening authority and, if appropriate, action of officer exercising general court-martial jurisdiction.
- f. Exhibits admitted in evidence.
- g. Exhibits not received in evidence. The page of the record of trial where each exhibit was offered and rejected will be noted on the front of each exhibit.
- h. Appellate exhibits, such as proposed instructions, written offers of proof or preliminary evidence (real or documentary), and briefs of counsel submitted at trial.